S. HRG. 106–64

MEDICAL RECORDS CONFIDENTIALITY IN A CHANGING HEALTH CARE ENVIRONMENT

HEARING

OF THE

COMMITTEE ON HEALTH, EDUCATION, LABOR, AND PENSIONS UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

ON

EXAMINING ISSUES RELATING TO MEDICAL RECORDS CONFIDENTIALITY IN A CHANGING HEALTH CARE ENVIRONMENT, AND RELATED MEASURES INCLUDING S. 881 AND S. 578, BILLS TO ENSURE CONFIDENTIALITY WITH RESPECT TO MEDICAL RECORDS AND HEALTH CARE-RELATED INFORMATION

APRIL 27, 1999

Printed for the use of the Committee on Health, Education, Labor, and Pensions

U.S. GOVERNMENT PRINTING OFFICE
56–463 CC WASHINGTON : 1999

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-058703-4

COMMITTEE ON HEALTH, EDUCATION, LABOR, AND PENSIONS

JAMES M. JEFFORDS, Vermont, *Chairman*

JUDD GREGG, New Hampshire
BILL FRIST, Tennessee
MIKE DeWINE, Ohio
MICHAEL B. ENZI, Wyoming
TIM HUTCHINSON, Arkansas
SUSAN M. COLLINS, Maine
SAM BROWNBACK, Kansas
CHUCK HAGEL, Nebraska
JEFF SESSIONS, Alabama

EDWARD M. KENNEDY, Massachusetts
CHRISTOPHER J. DODD, Connecticut
TOM HARKIN, Iowa
BARBARA A. MIKULSKI, Maryland
JEFF BINGAMAN, New Mexico
PAUL D. WELLSTONE, Minnesota
PATTY MURRAY, Washington
JACK REED, Rhode Island

MARK E. POWDEN, *Staff Director*
SUSAN K. HATTAN, *Deputy Staff Director*
J. MICHAEL MYERS, *Minority Staff Director and Chief Counsel*

Public laws/Hearings/Senate/106th Congress/1st session/1999

CONTENTS

STATEMENTS

TUESDAY, APRIL 27, 1999

	Page
Jeffords, Hon. James M., Chairman, Committee on Health, Education, Labor, and Pensions, opening statement	1
Kennedy, Hon. Edward M., a U.S. Senator from the State of Massachusetts, opening statement	2
Prepared statement	3
Bennett, Hon. Robert F., a U.S. Senator from the State of Utah; and Hon. Patrick J. Leahy, a U.S. Senator from the State of Vermont	5
Prepared statement of Senator Leahy	9
Dodd, Hon. Christopher J., a U.S. Senator from the State of Connecticut, prepared statement	18
Bentivoglio, John T., Special Counsel for Health Care Fraud, Office of Deputy Attorney General, U.S. Department of Justice, Washington, DC, accompanied by Lynne A. Hunt, Chief, Financial Crimes Section, Federal Bureau of Investigation	20
Prepared statement of Mr. Bentivoglio	22
Weich, Ronald H., Zuckerman, Spaeder, Goldstein, Taylor & Kolker, Washington, DC, on behalf of the American Civil Liberties Union; and Robyn S. Shapiro, director, Center for the Study of Bioethics, Medical College of Wisconsin, Milwaukee, WI, on behalf of the American Bar Association	37
Prepared statements of:	
Mr. Weich	39
Ms. Shapiro	50
Shedor, LaDonna, chief information officer and director of management information systems, Centra Health, Lynchburg, VA, on behalf of the Healthcare Leadership Council; and Dr. Paul Appelbaum, chairman, department of psychiatry, and director, law and psychiatry program, University of Massachusetts Medical School, Worcester, MA, on behalf of the American Psychiatric Associattion	60
Prepared statements of:	
Ms. Shedor	62
Dr. Appelbaum	66
Curd, Dr. John G., vice president of clinical development, Genentech, Inc., San Francisco, CA; and Chris Koyanagi, director of legislative policy, Judge David L. Bazelon Center for Mental Health Law, Washington, DC, on behalf of the Consumer Coalition for Health Privacy	72
Prepared statements of:	
Dr. Curd	76
Ms. Koyanagi	81
Hagel, Hon. Chuck, a U.S. Senator from the State of Nebraska, prepared statement	90
American Psychoanalytic Association, Robert Pyles, president, prepared statement	91
National Association of Insurance Commissioners, Kathryn Sebelius, Insurance Commissioner, prepared statement	105
The Washington Business Group on Health, prepared statement	109

ADDITIONAL MATERIAL

Articles, publications, letters, etc.:	
Questions from Senator Wellstone with responses from Ronald Weich	46
Privacy Principals, from the Amerian Psychoanalytic Association	95
Questions asked by Senator Wellstone with responses by Ms. Koyanagi	115
Questions asked by Senator DeWine with responses from Ms. Shapiro	116
Questions asked by Senator Wellstone with responses by Ms. Shapiro	117
Questions asked by Senator Wellstone with responses by Dr. Appelbaum	118

MEDICAL RECORDS CONFIDENTIALITY IN A CHANGING HEALTH CARE ENVIRONMENT

TUESDAY, APRIL 27, 1999

U.S. SENATE,
COMMITTEE ON HEALTH, EDUCATION, LABOR, AND PENSIONS,
Washington, DC.

The committee met, pursuant to notice, at 9:34 a.m., in room SD–628, Dirksen Senate Office Building, Senator Jeffords (chairman of the committee) presiding.

Present: Senators Jeffords, Frist, Hutchinson, Collins, Kennedy, Dodd, Wellstone, Murray, and Reed.

OPENING STATEMENT OF SENATOR JEFFORDS

The CHAIRMAN. Good morning. Today marks the Health and Education Committee's seventh hearing on one of the most pressing issues confronting our health care system—the confidentiality of health care information.

At today's hearing, we will be examining the topics of law enforcement, authorization, and preemption as they pertain to patient confidentiality.

This series of hearings has provided committee members with a better understanding of the complex issues surrounding the use of health care information and has given us a clear sense of the need for Federal legislation.

The current loose web of medical records protections at the Federal and State levels which has evolved in the absence of a comprehensive law leaves many aspects of health information unevenly protected. If Congress fails to enact Federal privacy legislation by August 21, 1999, the Secretary of Health and Human Services is required, according to the Health Insurance Portability and Accountability Act of 1996, or HIPAA, to promulgate regulations establishing electronic privacy standards on February 21, 2000. With that deadline only months away, we have our work cut out for us.

Recently, along with Senator Dodd, I introduced S. 578, bipartisan legislation to establish necessary national standards to protect the confidentiality of each American's medical records. In addition, Senators Leahy and Kennedy have introduced S. 573, medical records privacy legislation; and yesterday, Senator Bennett introduced the Medical Information Protection Act. All three of these bills have been referred to the committee for our consideration.

In order to meet the HIPAA deadline, I am planning to hold a committee markup on health information confidentiality legislation next month. In developing the legislation for markup, I intend to

draw from the best provisions of the three medical records bills that have been referred to the committee.

The time is ripe for action. Major technological advances in health care administration, delivery and payment systems have greatly improved the quality of patient care. However, we must also have guarantees to protect the privacy of every American's medical records.

A recent study by the National Research Council shows that the pathway of a typical medical record is no longer confined within the control of the patient's personal physician. Today, records may be handled by numerous individuals in more than 17 different organizations.

Quality care requires more than the free flow of information among providers, payers and other users of health information. It requires trust between a patient and a caregiver. Patients must feel comfortable sharing sensitive information with health professionals.

Technology has provided the tools to allow the ease of access to health care information. Now legislation is needed to ensure the confidentiality of this personal form of information.

Today we will be hearing from Senator Bennett and Senator Leahy, two distinguished colleagues of mine who have been leaders on the medical records privacy issue, as well as from other experts on the issues of law enforcement, authorization, and preemption.

The hearing will follow the committee's usual format. Each witness will speak for 5 minutes, and each Member will have up to 5 minutes per round for questioning. The hearing record will remain open for 2 weeks, and any written statements and questions for the record should be submitted within that time frame.

That said, let me welcome all the witnesses. I look forward to hearing your testimony.

I now turn to my good friend, Senator Kennedy.

Opening Statement of Senator Kennedy

Senator KENNEDY. Thank you very much, Mr. Chairman. I want to express all of our appreciation for the hearings that we have had on this subject matter, which is of enormous importance to families all over this country. The way that these hearings have been structured has really maximized our committee's, and hopefully the public's understanding of this issue. As you pointed out in your opening comment, we have more privacy when we rent a video at Blockbuster than we have in terms of medical records. It is a startling but true fact.

Americans are naturally concerned about this. They are concerned, as we have heard over the course of our hearings, that they are not going to have privacy protections, and then, clearly, they are not going to give the kind of information to their doctors that they should give in order to be able to get the best medical attention—or they will lie to the doctor if they have a sense that the information is going to be shared and may very well impact their employment or whether they will be able to get health insurance.

We want to try to make sure there is a balance between the providers of health care and those in the health care industry to enhance their ability to improve health care delivery service. There

must be some degree of flexibility so the providers themselves are able to gain information and give the best health care to their patients.

I want to thank Senator Leahy for his leadership as a key member, along with others on the Judiciary committee, for having been enormously involved in the protection of individuals' privacy issues and individuals' rights. As a former prosecutor, working with him, we have gained a great deal in terms of also balancing the legitimate interests of law enforcement and establishing a reasonable standard. We will have a chance to get into some of these issues today.

We have also incorporated many of the well-tested ideas on health research at the National Institutes of Health.

I join Senator Leahy in supporting legislation that today has the broad support of over 100 different organizations, including researchers and patient organizations, consumer organizations, and providers. We have been heartened working with them to have their support.

Finally, Mr. Chairman, we have tried to be sensitive to those States that have particular needs. We have tried to establish a floor so that Americans across the country will know whether in this Nation that their medical records will be protected but also to permit the States to take some opportunity to meet very special needs.

So we, Mr. Chairman, want you to know that we are looking forward to working with you and with other members of the committee. It is enormously important, as you have pointed out. We do not want to let this just drift into being an issue dealt with by administrative fiat. As much as we respect—and all of us do—the extraordinary leadership of Secretary Shalala and the administration, we should be the ones who decide the policy, and we are looking forward to working with you and Senator Bennett and our colleague Senators Dodd and Frist and other members who are here today to try to get good legislation that will meet these conflicting needs but do it in ways which will have broad support.

Thank you, Mr. Chairman.

[The prepared statement of Senator Kennedy follows:]

Prepared Statement of Senator Kennedy

It is clear that Congress needs to act to provide greater protection for the privacy of medical records. It is a national scandal that video rental records today have greater protection than sensitive medical information.

The privacy of personal medical information is an increasingly important issue in today's rapidly changing health care system. Congress recognized the need to protect the privacy of medical information when it passed the Kassebaum-Kennedy Act in 1996. That legislation contained a provision requiring Congress to enact privacy legislation by August of this year. If the deadline is not met, the Administration is required to issue regulations to protect the privacy of electronic records. However, those regulations would not apply to paper-based medical records. We know that the great majority of medical records are on paper. In fact, Congress has a

responsibility to enact strong privacy protections for all medical records.

In order to meet this challenge, Senator Leahy and I have introduced the Medical Information Privacy and Security Act. Our proposal, which establishes safeguards to protect private medical information and strengthens the confidential relationship between patients and physicians, is supported by more than 100 consumer, provider, and civil liberties organizations.

Patients who are concerned about their privacy are less likely to disclose important information to their physicians. According to a recent survey by the California HealthCare Foundation, one in six adults has taken extreme steps to protect their personal medical information, such as asking physicians to exclude information from their records, and even lying about their medical history. To succeed in improving the quality of health care in this country, we must ensure that patients can be open and honest with their physicians, without fear of privacy violations.

The legislation we are proposing recognizes the fundamental right of patients to limit disclosure of personally-identifiable medical information. We have balanced that right with the needs of providers and health care plans to use medical information to improve patient care. Our proposal does not force patients to sign a blanket authorization in order to receive care. Instead, it contains a flexible framework that can be modified to fit different situations.

Our proposal also builds upon the privacy protections currently assured for patients and their medical information in federally-funded research, and extends the protections to those who participate in other health research as well. Patients deserve to be assured that their information will be protected and treated with respect if it is used for research purposes. Patients must not lose faith in the integrity of the research process in this period of landmark breakthroughs.

In addition, our legislation allows states to grant additional protections to patients, beyond the Federal standard established in the bill. Many States have passed privacy laws or are currently considering legislation, and it is important to allow them to address privacy issues as they arise in this rapidly evolving area.

Further, as a general principle, our legislation requires law enforcement officials to obtain a warrant, subpoena, or court order before obtaining access to private medical records.

Congress must act now to address these important issues, and I am optimistic that we will meet the August deadline. I look forward to the testimony of our witnesses. I also extend a special welcome to Dr. Paul Appelbaum, the Chairman of the Department of Psychiatry and Director of the Law and Psychiatry Program at the University of Massachusetts Medical School in Worcester, MA.

The CHAIRMAN. Thank you for an excellent statement.

I will say that it is a real challenge to have 5 Senators—6, really—actively working on this bill but with different ideas. So it is going to be a challenge, but I am very pleased with the efforts of all of those who are participating to try to find a consensus here.

I am pleased to welcome 5 panels of witnesses this morning who will share their expertise with the committee also.

First, it gives me great pleasure to introduce 2 distinguished colleagues of mine, Senator Robert Bennett and Senator Patrick Leahy, who have been leaders on this issue of medial records privacy for some time. I am delighted that they could both be with us this morning to share their thoughts.

Please proceed.

Senator KENNEDY. Mr. Chairman, I hope to be here to hear the testimony of Dr. Paul Appelbaum, who is chairman of the Department of Psychiatry and director of the Law and Psychiatry Program at the University of Massachusetts Medical School in Worcester. I want to extend a very warm welcome to him. As the chair knows, we are marking up the bankruptcy legislation and also, in the Armed Services Committee, matters dealing with Kosovo, so I will do my best to be here, but I wanted to express appreciation to the committee for inviting Dr. Appelbaum.

Thank you very much.

The CHAIRMAN. Thank you.

Senator Bennett.

STATEMENTS OF HON. ROBERT F. BENNETT, A U.S. SENATOR FROM THE STATE OF UTAH; AND HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Senator BENNETT. Thank you very much, Mr. Chairman. I want to thank you for holding the hearing and for your role in this important issue of protecting personal identifiable health information.

I am pleased to be here to talk about the subjects you have identified for today's hearing—Federal preemption, the consolidated authorization, and law enforcement's ability to access medial records. Each of the areas is an important aspect of any legislative effort to provide appropriate protections for our medical information.

Before I get into the issue of Federal preemption, let me make a personal statement. People keep asking me as a conservative Republican who believes in States' rights and States' preeminence, how can you come out in favor of Federal preemption.

I want to assure you and the committee that I have not approached this issue from the standpoint of political ideology but out of my background as a manager, I have come to the conclusion from a straight managerial point of view that the logical thing is to have Federal preemption of State law. I think it is vital.

Most of us wrongly assume that our personal health information is already protected under Federal law. As Senator Kennedy has noted, it is not. Federal law protects the confidentiality of our video rental records and Federal law ensures us access to information about ourselves such as our credit history, but there is no current Federal law which will protect the confidentiality of our medical information against unauthorized use and ensure us access to that same sensitive information about us. It is ironic that other people can see the information but we ourselves cannot in many situations.

Delivery of health care is a matter of interstate commerce. No longer are one's health care needs met within State boundaries. We consult specialists in other States. We are engaged in telemedicine, and health systems services very often straddle State lines.

All Americans should have the assurance that their medical records are being treated with the same appropriate safeguards and dignity that they deserve. This patchwork of State laws is confusing, contradictory and complex. Individuals, providers, insurers, health plans and others are forced to deal with this maze of State laws which fail in many cases to provide the needed and desired protections. A Federal floor provides only temporary relief from this maze of State laws. Soon, some States will pass a new law that will once again create confusion and slow the advancement of health care delivery and research.

I see no compelling reason to pass medical records protection legislation if there is not full and complete Federal preemption. What would be the point? We would only find ourselves in a similar to the one in which we find ourselves today—a patchwork of State law.

I believe that all individuals should have the right and the ability to sign an authorization form. Each of us should have a better understanding as to how and for what medical information is being used. I do not believe that we need to, as many of us do today, sign authorizing forms each and every time we receive care from a different doctor or nurse. I believe we should not be forced to agree to other activities outside of treatment, payment and health care operations in order to receive treatment. When someone wants to use our medical information for marketing purposes, we should have the ability to say, "No, thank you." We should have the right to revoke our authorization but in doing so realize that with such a revocation, there are consequences and that we cannot expect our health care providers to provide us with the treatment when they only have access to a portion of our records. To do so puts our health at risk and places are caregivers in a precarious situation where they cannot hope to render the appropriate care.

Finally, I would like to address the issue of law enforcement. There are times when in the course of their duty, law enforcement officials need access to medical records. I believe it is in the best interest of the public to provide them with this access, but I believe we are better served when such requests are reviewed and authorized through an appropriate process.

My legislation would require either a warrant or a subpoena prior to law enforcement officials having access to anyone's medical records.

I am sure that law enforcement officials understand that there cannot be two standards when it comes to medical records. In order for individuals to have confidence in the system, there must be appropriate checks within the system in order to assure that all the information is required and that a legitimate need has been demonstrated.

I understand the unique nature of the law enforcement officials and believe we can come to a reasonable compromise regarding the privacy concerns of the individual and the legitimate needs of the law enforcement community.

Mr. Chairman, I look forward to working with you and the other members of this committee in crafting legislation that provides all Americans with greater access to their medical information as well as greater protection, and I thank you for your attention.

The CHAIRMAN. Thank you, Senator Bennett.

Next, my good friend from Vermont, Senator Leahy.

Senator LEAHY. I am glad to be here with Senator Bennett. I have noticed since the time he came to the Senate has strong interest in this subject, and I have enjoyed serving with him during the years that he has been here.

These issues are not new. In 1993, when I chaired the Judiciary Committee's Subcommittee on Technology and the Law, I convened hearings on the privacy of medical records and new technology. Senator Kennedy will remember that well, because he was of invaluable assistance in that. We learned a lot about how technology is overtaking our privacy rights. With the Information Age enthusiasm, it became clear to me that technology could be a powerful tool for protecting our privacy rights or could be a powerful agent in eroding them.

The question is whether we make it our servant or our master. In 1996 during consideration of the Kassebaum-Kennedy Health Insurance Portability Act, Senator Bennett and I worked very closely to include medical privacy protections in that law. In the end, what we were able to include is now the deadline that is looming. At a time when our leading computer chip and software companies have built secret identifiers into their products to trace our every move in cyberspace without our consent, we have to ask ourselves whether Congress can stand by and see the potential erosion of the public's medical privacy rights.

The ability to compile, store and cross-reference personal health information has made our intimate health history a valuable commodity. In 1996 alone, the health care industry spent an estimated $10 to $15 billion on new technology just to store and compile this material.

Mr. Chairman, you may remember the recent article from The Wall Street Journal which I cited at your Vermont field hearing in March about a company seeking the motherload in health data mining. This company wants to get health data on millions of Americans of all States and then sell it to the highest bidder. Today there are no laws constraining the creation of large databases filled with sensitive, personally identifiable information on any of us. Information on all of us, no matter how private, is like gold to these so-called data miners.

We have to make sure the grassroots stakes that our constituents have in these decisions is not overrun by the high-powered and well-funded lobbying efforts on these special interests who stand to make millions if they can just delve in and get Senator Collins', Senator Hutchinson's, Senator Frist's, Senator Jeffords', Senator Kennedy's, Senator Murray's, Senator Bennett's and Senator Leahy's medical records as well as everyone else's.

We must not let threats to privacy rise to the point where the only way a person can ensure confidentiality is to avoid seeking medical treatment in the first place. With some people, it may come to that—if they are afraid they cannot protect their privacy otherwise, they might not seek the medical care they need.

Mr. Chairman, you are working to try to bridge the gaps between the various legislative efforts to address this issue. I applaud you for that and look forward to working with you.

There are similarities between the bills that Senators Kennedy, Daschle, Dorgan and I have introduced, S. 573, MHPSA, and the bill that you and Senator Dodd introduced, and the legislation that Senator Bennett and Senator Mack introduced yesterday.

There is one area that has been used as a red herring by some of the special interests on the question of health research. They have used this charge as a red herring to try to kill the passage of any medical privacy law, or at least of any strong protections for health consumers.

But we all agree, all of us, that once medical information is identified for research or other purposes, it falls out of the scope of our legislation. The bill that Senator Kennedy and I introduced keeps in place the current review structure for health research at institutions using Federal funding, such as NIH. NIH is often touted, as well it should be, as the best health research institution in the world. So following their privacy methods, I do not see how that would in any way stifle research.

Other issues may not be so simple to resolve until we get to the Senate floor, such as preemption of State law. here again, we all agree that weaker health privacy laws should be preempted. The legislation which Senator Kennedy and I have introduced does not preempt any Federal or State law or regulation that offers greater privacy safeguards. And our legislation, which may differ, makes room for the many possible future threats to medical privacy that we do not anticipate today.

We have to understand that there is a lot of technology that, no matter how current we feel we are, we cannot predict. Even the best minds do not know where technology will be 10 years from now.

We have differences on the question of preemption. These are differences of opinion. But my view is that addressing concerns about medical privacy is not static. Preempting State consumer protection laws, for example, Congress has never done. For instance, consumer protections in financial and communications law set a Federal floor, not a preemptive ceiling. That is a precedent that we should follow.

In our own State, for example, we have a cancer registry which I have worked to help expand, as you have, to find a cure. The National Association of Insurance Commissioners point out that our State statute requires that the health commissioner keep confidential all information reported to the cancer registry with the exception of exchange of confidential information with other States' cancer registries.

Now, if we had a Federal law that preempted our State laws, we could argue that you could wipe out the Vermont Cancer Registry. We do not want to do that. The public's interests, not special interests, have to be paramount as we proceed, and it should not become a special-interest wish list or a partisan issue.

I believe that we can take these various bills and work together and craft a good piece of legislation which does not run roughshod over the States but does protect individual consumers of health care. If we do not, I guarantee you we will have thousands—millions—of Americans who will not seek health care because they will be afraid of what it might do to their privacy.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you both for excellent statements, and thank you for all the work you have done. I am confident, having worked with you and your staffs, that we are in a position to put together a bill that we will all be able to get behind, and that is certainly my goal.

[The prepared statement of Senator Leahy follows:]

Prepared Statement of Senator Leahy

Mr. Chairman, this is another Y2K Week in the Senate. But as you and I and others who have been in the trenches on the medical privacy issue know, the Millennium Bug is not the only computer-related problem Congress faces this year.

We are fast approaching the deadline that Congress set for itself of August 21 this year to solve the multitude of privacy glitches in the handling of our medical records——both electronic and paper-based.

If we do not act, this responsibility falls to the Secretary of Health and Human Services. Medical records privacy is public policy at an elemental level. Setting these standards is far too important to punt to the bureaucracy. Congress must make these choices.

The issues we face in passing legislation in this area are not new. In 1993, when I chaired the Judiciary Committee's Subcommittee on Technology and the Law, I convened hearings on the privacy of medical records and new technologies. We learned a great deal about how technology is overtaking our privacy rights.

As an Information Age enthusiast, it became clear to me that technology can become a powerful tool for protecting our privacy rights, or it can become a powerful agent in eroding them. The answer is in the choices we make in making technology our servant, instead of our master.

In 1996, during consideration of the Kassebaum/Kennedy health insurance portability bill, Senator Bennett and I worked very closely to include medical privacy protections in that law. In the end, what we were able to include is the deadline for action that is now looming.

At a time when our leading computer chip and software companies have built secret identifiers into their products to trace our every move in cyberspace without our consent, it is time for Congress to wake up to the erosion of the public's medical privacy rights. The ability to compile, store and cross reference personal health information has made our intimate health history a valuable commodity. In 1996 alone, the health care industry spent an estimated $10 to $15 billion on information technology.

Mr. Chairman, you may remember the recent article from The Wall Street Journal that I cited at the Vermont field hearing you held in March, about a company that is "seeking the mother lode in health data mining." This company wants to get medical data on millions of Americans to sell to other companies. Today there are no laws constraining the creation of large privately-owned medical data bases filled with sensitive personally identifiable information on any of us. Information on all of us, no matter how private, is like gold to these "data miners."

As Congress works toward passing legislation, the privacy interests of the American public will be at odds with powerful economic interests and with the penchant of large organizations and complex systems to control this kind of personal information. Well-funded and sharply focused special interests often win in a match-up like this. We must work together to make sure that the grassroots stake that our constituents have in these decisions is not over-run by the high-powered and well-funded lobbying efforts of these special interests. We must not let threats to privacy rise to the point that the only way for a person to ensure confidentiality is to avoid seeking medical treatment.

Mr. Chairman, under your leadership the work is underway to try to bridge the gaps between our legislative efforts to address this issue. I look forward to seeing the product of your committee's work in this area. I certainly offer any assistance that I or my staff can provide in ironing out some of the differences in our respective bills before this issue reaches the Senate floor for debate.

There are many similarities between the bill that Senators Kennedy, Daschle, Dorgan and I introduced, which is S. 573, the Medical Information Privacy and Security Act (MIPSA), the bill that you and Senator Dodd introduced, and the legislation that Senators Bennett and Mack introduced.

In addition to similar provisions there are also several nuanced differences that I believe can be easily resolved. An issue I include in this category, which might surprise you considering some of the rhetoric that is sometimes thrown around these hallways, is health research. Some special interests have used the very impor-

tant issue of health research as a red herring to try to kill the passage of any medical privacy law, or at least to kill any strong protections for consumers.

We all support health research. We all agree that once medical information is de-identified for, research or any other purpose it falls out of the scope our of legislation.

The bill Senator Kennedy and I introduced keeps in place the current review structure for health research at institutions using federal funding, such as NIH. We ask the Secretary of Health and Human Services to examine whether this system can be improved. We also extend the review structure, and its consumer protection components, to privately funded research.

The NIH is often invoked, and I believe rightly so, as the best health research institution in the world—so I would like to hear a reasonable argument as to why following its privacy methods would be stifling to other research.

Another issue that has been used as a red herring is the idea of "single" versus "multiple" authorizations from patients for treatment, payment and other uses of identifiable health information. All of the bills before the Senate allow for a single authorization for treatment and payment. Where we differ, and I do believe we can find agreement on an appropriate policy, is the exception in the other bills for "health care operations." At present, however, this newly invented term is far too broad in scope and does not include the necessary accountability measures to protect against anyone from calling their activity using identifiable data a "health care operation" and getting around the spirit of the law.

None of us want to stop the ability of a health provider or health facility to provide effective health care. But those in the health care industry that are seeking this broad escape clause from patient privacy protections must justify the need for complete datasets of identifiable information for this broad range of management functions. At present they have not.

We all agree that uses of medical information outside the scope of treatment and payment and possible management functions that are not related to the provision of care for patients would require additional authorization.

Standards for law enforcement access to medical records is another area where we all seem to be in basic agreement. We may differ in our exact approach, but I hope with the constructive input of the U.S. Department of Justice we can effectively balance the privacy rights of individuals and the sometimes urgent need for law enforcement access to this information.

Other issues may not be so simple to resolve except on the Senate floor, such as preemption of state law. We all agree, however, that "weaker" health privacy laws should be pre-empted. So by virtue of passing a federal law we are going to foster a great deal of the uniformity that the health care industry is seeking.

Mr. Chairman, the bill you have introduced, cosponsored by Senator Dodd, and the bill that Senator Bennett has introduced address the issue of preemption differently. While I respect that we have differences of opinion, my view is that addressing concerns about medical privacy is not static. Preempting state consumer protection law is not the way Congress has dealt with this type of issue in the past. For instance, consumer protections in financial and communications law set a federal floor—not a pre-emptive ceiling. The legislation we enact should not change this precedent.

The legislation that Senator Kennedy and I introduced does not preempt any federal or state law or regulation that offers greater privacy safeguards. We propose a floor rather than a ceiling, achieving two goals:

First, as I mentioned, having a federal privacy floor will eliminate much of the current patchwork of state laws governing the exchange of medical information, and will replace the patchwork with strong, clear, basic standards that will apply to everyone.

Second, and this is where we differ, MIPSA makes room for the many possible future threats to medical privacy that we may not even anticipate today. As medical and information technology moves forward into the next century we must maintain the public's right to meet future technological challenges to privacy with stronger medical privacy laws closer to home.

I am amazed by an argument used in support of preempting stronger state law. It seems that now, if someone disagrees with a strong consumer protection statute in a particular state that the answer is to come to the federal level and ask us to pass a weaker law and preempt the stronger state law. The idea that we should start encouraging our constituents to come to us at the federal level anytime they disagree with a strong state consumer protection law and we will just wipe out the work and expressed interests of states is incredulous.

In our home state of Vermont, like many other states, we have a cancer registry, which I have worked to expand as a tool to help find a cure for this dreadful dis-

ease. The National Association of Insurance Commissioners has pointed out that our state statute requires that the Health Commissioner keep confidential all information reported to the cancer registry, with exceptions for the exchange of confidential information with other states' cancer registries, federal cancer control agencies, and health researchers, under specified conditions.

The provisions of this Vermont law arguably would be overridden by a federal privacy law that totally preempted state law or did not include state cancer registry laws as an exception to federal preemption.

In my experience it is usually the case that the best ideas for federal laws in any area begin in the states. Preempting the ability of states to address medical privacy concerns that will arise in the future—either because technology has changed, or by virtue of a fact that no federal law is going to be perfect—is wrongheaded. We must continue to allow states to be the laboratories for progress and innovation.

Mr. Chairman, I have testified before this committee many times so I will not again elaborate on the need for comprehensive federal medical privacy legislation. By now, the need should be clear.

My message today is that we must act now. The public's interests—not special interests—must be paramount as we proceed. Passing medical privacy legislation is too important to allow it to become a special interest wish list or a partisan issue.

The CHAIRMAM. Senator Kennedy.

Senator KENNEDY. Just briefly, I want to thank both of you. In this circumstance, Mr. Chairman, both of our colleagues have a good grasp and understanding of the legislation and long-held views, and I think they are highly respected positions in terms of the pressures that all of us have in terms of trying to work this process through.

I would ask Senator Bennett about one aspect of the legislation and perhaps you would like to submit some additional information. I have tried to lay out the different pieces of legislation and the five major areas and compare the similarities to see if we cannot find some common ground. In your legislation as well as in the Jeffords-Dodd proposal, under the required authorization, you use the words "health care operations related to disclosures." Among other provisions, it "requires one-time authorization for treatment payment," and "health care operations." And then it allows patients to self-pay to avoid payment-related disclosures, which has been a real problem for many people. "Other disclosures require authorization separate from treatment and payment authorization and cannot condition care upon receipt." Those are certainly important points, but the "health care operations" at least lends itself to I would imagine a variety of different operations.

I do not know whether you have thought through about what fits within that definition, how you would define it, or if it is something you could provide to us after the hearing, so we can have a pretty good idea, because this is obviously one area where yours is different from some of the other proposals that we have before us.

Senator BENNETT. Surely. I will be happy to provide specific details and background.

Let me give you the overall background for why that is in. When I first got involved in this issue close to 4 years ago and introduced the first piece of legislation with my name on it—and Senator Leahy was at that time a cosponsor of it—this was not included, and in the subsequent 3½ to 4 years that I have spent working on this issue, my door has been open to anybody who is affected by this to come in and tell us specifically how it would impact, and in the process of that information-gathering activity, a number of health providers came in and said: You have so narrowly focused on just treatment and payment that you have overlooked the im-

pact of your legislation on our ability to run a hospital. We have to have access to some of this information to make routine operational decisions.

And I said, as I have said here today, I have no ideological commitment on this bill. I want us to solve the managerial problem, and I do not want to get in the way of somebody who has legitimate managerial reasons to have access to this information. Come and tell us what you need.

So a number of health care providers literally over the years, because as I said, we have been involved in this thing for several years now, have met with my staff, have given us examples of legitimate uses of this activity in order for them to manage their facility, and it is in response to that kind of information gathering that we put this language in the bill. Senator Jeffords and Senator Dodd have been aware of this, and that is why similar language is in their bill. We will be happy to provide the committee with specific information.

This is not an attempt to do anything other than make sure the normal operations of a legitimate health care provider are not interfered with in a way that would otherwise damage the delivery of services to a patient.

Senator KENNEDY. Perhaps we could at least gain some additional insight. The concern, as you can probably imagine, is that some plans would claim that any activity they undertake is really a "health care operation," and they would expand those words to have somewhat different—it could mean any kind of information or transaction, could it not?

Senator BENNETT. We believe that we have addressed those concerns. They are legitimate concerns, and they ere raised in my office when these first questions came in. I will be happy to supply to the committee all the background that we have in this area.

Senator KENNEDY. Thank you.

Finally, your legislation effectively preempts the States and virtually prohibits the States from acting further. Given the technological breakthroughs that we are seeing today—with the use of the internet, for example, in prescribing drugs—isn't that fairly prescriptive in terms of the future and the possibilities in terms of new kinds of technology and new ways of delivering services as well as new kinds of diseases and treatments and needs?

Senator BENNETT. In my opinion, the language would not prohibit any progress in those areas, and I would suggest to you, sir, that if you allow the States to respond to those on a patchwork kind of basis rather than let the Federal Government respond to those breakthroughs on a uniform basis, you could well have a circumstance where one State says this is how we are going to respond to this new breakthrough with this kind of legislation, and another State right next to it says, no, we think you are wrong on that, and they adopt a different standard, and the health care provider servicing people who live on that State line—and 50 percent of Americans do live on a State line and are constantly crossing back and forth—find themselves whipsawed between those two different approaches.

Again, I get the criticism from time to time that, gee, you are a conservative Republican, and you believe in States' laws and you

believe in State experimentation and letting the States be the laboratories, and I do ideologically believe in all of those things. But something that is scientifically based rather than ideologically based like this, I think should have uniformity nationwide. And if you get a breakthrough that requires a change in the standard, I am assuming that Federal officials are intelligent enough to make those changes, at least as intelligent as the State people, and could do it in such a way that would be uniform throughout the entire country.

Right now, if I might take my own State of Utah, which has no legislation at all on this issue, we happen to have very good practice because the standards have been imposed by the providers themselves, and the providers themselves have a high standard of good practice, and I do not feel particularly threatened by the absence of State law in the State of Utah, but I recognize that there is a great possibility that something done in another State or something done nationally could affect the practice in my State, and the health care providers in my State, who have thrived in this area without any legislation at all, have now come around and told me they support Federal preemption simply because they want a degree of uniformity and predictability in this area which currently does not exist.

Senator KENNEDY. I would just make a last comment. This is obviously the balance which I think Senator Leahy and I tried to get, where you establish a floor by which we establish the basic and fundamental kinds of protections and permit flexibility in terms of some States that want to enhance or provide additional protections. I think that that is at least somewhat a different view than you have.

I do not know if Senator Leahy wants to make a brief comment. I thank the chair very much.

Senator LEAHY. Senator Bennett had talked about there being a difference between whether it is scientifically or ideologically driven, and I would agree with him on that in concept. The trouble is sometimes determining where science stops and ideology takes over.

I mentioned in my testimony that red herring that has been brought up by some who say that our legislation would stifle research when we have had privacy guarantees. Well, unfortunately, some of the people who are saying you might stifle research ignore the fact that there are very strong privacy standards by NIH and others, but they are also doing the mantra of some of these data-mining companies, those that want to be able to go in and get all this data and sell it—your personal information—for a number of reasons. We saw this in this area with one of the local pharmacies as people suddenly began receiving all kinds of ads and so on, and it turned out that people's prescription information, which may reflect intimate facts about them, was being combined with information held by another company.

These are things that I think most of us find very worrisome. So if it were purely technology or purely ideology, it would be easy to make that cut, but I think that having a floor there helps us in

those areas where it is a question about what is technology and what is ideology.

The CHAIRMAN. Senator Frist.

Senator FRIST. Thank you, Mr. Chairman. I will be brief. I know we have five panels today.

I just want to make two points. One is to thank both of you for your tremendous leadership. Since I have been in the U.S. Senate for the last 4-1/2 years, the two of you, along with the ranking member and our chairman, have participated actively in discussions which strike right at the heart of the current practice of medicine but will also affect the future practice of medicine care that we will receive and our children will receive.

It has been fascinating because the debate comes down to the three fundamental issues we will be talking about today, and although today we are not talking quite as much about the research end of things, it is clearly very important. I feel very good that we can meet the August deadline because of the great work that the two of you especially have done.

My second and last point is that last night, my youngest son Brian, who is 11, had to memorize the Hippocratic Oath for school. He did not have to memorize the whole things; it has three sections. It is referred to a lot when we talk about the history of medicine and health care. Some people say it is outdated, but it really boils down to the tremendous importance and value of confidentiality and of the trust that has got to be at the heart of our debate today. That trust is reflected in the privacy issues which we all feel strongly about; trust in the future in terms of access to data and this balancing act that comes in in terms of the use of that data for the future; and then, as Senator Kennedy pointed out, this whole system is changing so fast, and we do not want to do anything that will lock us back in time as we go forward. But the Hippocratic Oath relates to the trust that, when you go to see a health professional, that information will be used principally in your best interest, number one, and number two, that if possible, it can be used for the interest of others in a way that you are very comfortable with. That is a balancing act that we must all go ahead with, and it comes back to something that does affect the quality of health care as a physician, and it goes back to that Hippocratic Oath. We will have time to go further into the three issues during the course of the debate, but I just want to thank you for your leadership.

Thank you, Mr. Chairman.

The CHAIRMAN. Senator Murray.

Senator MURRAY. Thank you, Mr. Chairman. I know you want to get on to the panelists.

Let me just thank you for having this hearing and thank both Senators Leahy and Bennett for their work on this issue. It is a difficult issue, and I think the key issues have already been talked about—the whole issue about whether the States, which have done a lot of work on this, ought to be able to continue to move forward and how we balance that, I think is key, and how we deal with the research issue versus patient rights.

I share Senator Leahy's concern that people will not seek medical help if they fear that they will not have the protection of privacy.

I have already talked to individuals who have not sought mental health services because they fear someone will find out about that. I am well aware that some insurance companies deny both life insurance and disability insurance to victims of domestic violence and women not seeking care for abuse because they are fearful that they will then be denied insurance coverage in the future.

These issues are difficult to balance against the needs of research, and I hear from my research committee as well. We have a lot of work to move through, and I appreciate both of you and your tremendous work on this and look forward to the panelists talking about how we deal with those issues.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Murray.

Senator Hutchinson.

Senator HUTCHINSON. Thank you, Mr. Chairman.

I also want to thank you for your presentations today, and I look forward to hearing the panels on what is clearly one of the most pressing issues this committee will address this year.

Senator Leahy, I wonder if you could address the law enforcement issue. I think Senator Bennett said that a subpoena or a warrant is what he envisioned as far as what law enforcement would have to do to justify access to those records. How would your legislation address that issue?

Senator LEAHY. We do the same thing. We have very strong law enforcement records. We know that law enforcement is necessary. I think the Secretary of HHS had wanted complete and unfettered access by law enforcement. We require a warrant or a grand jury subpoena or a court order.

Basically, what we are saying is this. We are saying that they have got to have the same kind of court proceeding as they would to get your video records. Alan Simpson and I wrote the so-called Bork law which we put in because of our outrage at somebody who had gone into former Judge Bork's video rental records and was publicizing them during his confirmation hearing. Senator Simpson and I wrote a law that said you could not do that. We felt that you ought to have at least as much protection of your very personal medical records as you do in regard to whether you rent "Star Wars" or not. It seemed to make sense that you would have at least that much.

As a former prosecutor, we had to get subpoenas or a search warrant to get somebody's medical records, and I did that in cases where it was appropriate. Law enforcement should have to do that whether your records are in electronic form or however they might be kept.

I do not think doctors are going to put much into a medical record if they think there is not at least that kind of privacy protection, but it would not stop law enforcement with the appropriate either search warrant or subpoena.

Senator HUTCHINSON. Thank you.

Senator Bennett, would you respond to that also and the concern that without unfettered access, it would unduly hamper law enforcement efforts on fraud and abuse and other needs for medical records?

Senator BENNETT. We have spent a lot of time working with the law enforcement community to come up with the right balance here, and we feel that we have struck it. There is, of course, very legitimate reason for law enforcement to have access to medical records, but they must be able to demonstrate it. We think we have found the right balance in the language that we have adopted. This has been a very difficult one that we have been working on for the period of time that I have talked about.

Senator LEAHY. I thought, for example, if you have been to a psychiatrist and have had psychiatric work and so on, that you should be entitled to at least the same privacy as whether you rented "Gone With the Wind."

Senator HUTCHINSON. It seems like a pretty compelling and logical argument to me. I am interested to hear why the concerns about even those kinds of limitations.

Thank you, Mr. Chairman.

The CHAIRMAN. Senator Wellstone.

Senator WELLSTONE. Thank you, Mr. Chairman.

I apologize that I did not get to hear either one of my colleagues, so I would just thank both of them and signal one big concern that I have. It is not so much in the form of a question, but it is to Senator Bennett, whom I have come to really appreciate.

On the issue of preemption of State efforts—in the State of Minnesota, we have a really strong piece of legislation which really goes to the heart of giving people some protections. We have made some adjustments to accommodate some people who have been doing medical research and we found a good balance. But I would find it very difficult—and I think this is the strength of your approach, Senator Leahy—to support something that would preempt what Minnesota has done. I am sure you are hearing that from other colleagues, and you might want to consider it as you go forward. But we have worked pretty hard in our State to get it right, and I would not want to see legislation that would preempt what I think is a really strong State effort.

Senator BENNETT. I addressed that before you came in, but let me say again—you cited your State, and let me cite my own, which has no State law whatsoever but has very good practice, and it has been put in place by the providers themselves, who recognize the importance of confidentiality. We have had little or no concern with respect to confidentiality within the State of Utah. Nonetheless they are wiling to give up the flexibility that they have, knowing that they can provide good practice in return for uniformity, because the problem that we run into with 50 percent of Americans living on State lines and having different standards back and forth across the State lines is a desire for uniformity here. As we move further into the Information Age, and this information goes around the country literally at the speed of light, it become very difficult for somebody to say we are going to comply with this State law here, the other State law there, and the established practice that is not mandated by law in another State. It becomes a patchwork that is almost impossible to deal with.

Senator WELLSTONE. I appreciate your comment. I guess my philosophy when it comes to which side you err on in these matters is that I think this has become such an important issue to families,

and I would prefer to establish the uniformity in terms of minimum standard, but I think that States that want to go forward and do even better should be allowed to do so. I am just saying that I believe that is the position of people in Minnesota, and that will be my position, understanding full well and holding respect for your position.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Wellstone.

Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

I want to join in commending our two witnesses for their leadership in this area as well as the leadership of several members of this committee. I think it contrasts very sharply with the lack of leadership by the administration in trying to come forward with a proposal that would strike an appropriate balance particularly in dealing with the law enforcement concerns that privacy legislation raises.

The rapid changes in the way in which health care has been provided, documented and paid for in the United States has raised very serious concerns about medical privacy and the confidentiality of our records, and I think everyone here is committed to drafting legislation that provides the kinds of protections that all of us would want for our personal records.

I would just add a cautionary note. Last year, the State of Maine passed a medical privacy bill that everyone thought was the answer to this problem. It had widespread support among all the stakeholders; it passed the legislature very easily and was signed into law by the Governor. And this year when it went into effect, it was in effect for all of 2 weeks when there was an outcry at the unintended consequences of the legislation.

The result has been that the legislature unanimously voted to suspend the law until October 1st of this year. The Governor has signed that suspension into law, and everyone is back to scratch to start to try to piece together a workable law.

So I think that Maine's experience in this area shows how difficult it is to achieve workable legislation even though every, single person in this room shares the goal of protecting sensitive medical information and ensuring the confidentiality that gives trust to people in their relationships with health care providers.

So I want to thank you very much for your contributions to this debate, and I look forward to our deliberations.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Collins.

Senator Dodd.

Senator DODD. Thank you very much, Mr. Chairman.

I ask unanimous consent that my prepared remarks be included in the record.

Let me welcome our two colleagues who have worked very, very hard on this issue. Senator Bennett has been involved in this for a long time as has Senator Leahy, and their advice and counsel means an awful lot. In fact, Senator Jeffords and I, as I think all of you know, have introduced a bill, and we had a good conversation in fact the other day with Senator Bennett about some of his ideas on all of this.

Mr. Chairman, I want to thank you. Normally, in committees like this, we reauthorize legislation that is needed. Here, as Senator Collins' has just pointedly pointed out, we are sort of venturing into the unknown in an area where there are lots of consequences to this issue. There is an initial reaction to it which we can all appreciate, but there are the unintended consequences that can occur.

The only constituency that I know of that probably does not care about this so much are those who are operating under the false impression that they do not have a problem. If you look at what existing Federal law does today, there is absolutely no law that establishes an individual's right to privacy of sensitive medical information. Right now, you do not have a right to see your medical records, you do not have a right to keep your insurer from sharing your records with your employer, you do not have a right to prevent information you give to your doctor in confidence from being used in direct marketing. These are rights that people think they have but they do not.

So what we are obviously trying to do here, given the Information Age we are exploding into—and I have deep respect for what the States are doing, which our colleague from Minnesota articulated very well—what Senator Jeffords and I have tried to do is to combine both of those—to recognize the State effort, but to also have some appreciation that if we do not have a national standard in this area, it will be very, very difficult to have the kind of uniformity that is necessary to deal with it.

I think the committee members are aware of the sort of middle ground that we have carved out here as a way of trying to satisfy the desires at the State level to do something in this year while at the same time recognizing that there is a real need for a Federal role here given the magnitude of this problem, rather than a patchwork of laws across the country when it comes to these issues, if for no other reason than I think consumers would like to have clarity on this, as well as our researchers, our doctors, our insurers, our employers. Everyone needs clarity, and there is a danger when you run in the other direction here that you will lose that which will be critically important if this law or the proposals are going to succeed.

Today about 90 percent of all medical records are still in the old file cabinets. The assumption that it is all on computers is not the case. Ninety percent of it is in file cabinets. That is changing by the hour. To give you some idea, the volume on the internet doubles every 6 weeks. That is the explosive nature of the internet, and clearly, that is the direction in which this is going, and as a result, access to this information will be global in its perspective let alone national. So the need for national legislation in this area I think is obvious.

Again, Mr. Chairman, I thank you for your efforts and am deeply appreciative of the efforts of our two colleagues.

[The prepared statement of Senator Dodd follows:]

Prepared Statement of Senator Dodd

Mr. Chairman, I want to thank you for convening a hearing on this critical and timely topic. I also want to thank you for your

leadership on this issue and for making the privacy of medical information a top priority of the Health and Education Committee.

I also want to extend special thanks to Senators Bennett and Leahy for joining us. The committee owes both of you a debt of gratitude for your years of work on this issue. Without the groundwork laid by your advocacy, Congress's goal of enacting legislation before the August 1999 deadline would be pipe dream.

As all of you know, the Health and Education Committee has before it a challenge that rivals any it has yet encountered. As with most committees, the meat and potatoes work of the Health and Education Committee is the reauthorization and oversight of existing programs and laws. However, in this instance we are truly venturing into the unknown.

There is currently no Federal law that establishes an individual's right to privacy for sensitive medical information. And while some States have attempted to counter the most egregious violations of privacy, no State privacy law approaches the breadth and depth of what we are attempting here.

We must legislate for a future of highly advanced information systems at a time when the vast majority of medical records—by some accounts 90 percent—are still kept in paper form. We must devise commonsense rules to protect the use of medical information in research and health care delivery at a time when rapid evolutions in both areas are likely to render their current forms unrecognizable within a decade.

But, despite the sometimes overwhelming magnitude of the challenge, we are driven by the knowledge that the status quo is unacceptable.

The only people not yet concerned about the privacy of their medical records are those individuals still under the false impression that they actually have rights now. The fact is that right now you don't have the right to see your medical records. You don't have the right to keep your insurer from sharing your records with your employer. You don't have the right to prevent information you give in confidence to your doctor from being used for direct marketing.

By and large, with the exception of a few State laws, all you have standing between you and the misuse of your information are good intentions, professional ethics and internal company policies.

Senator Jeffords and I have been grappling with this issue since we first introduced the Personal Information Non-Disclosure Act last spring. And we are aware of the tough questions left to be resolved.

In February we heard a spirited debate over whether Federal oversight of health research should extend to research funded by the private sector. Today, we will examine: 1) how law enforcement officials should obtain access to medical information, 2) whether State laws should be pre-empted by the Federal law, and 3) how to design a workable process by which individuals authorize the use of their information.

These are all tough questions, but not insurmountable if we keep in mind that our constituents are unlikely to look kindly upon our failure to deliver the protections they are demanding.

With the assistance of Senators Leahy and Bennett and the commitment of the members of this committee, Chairman Jeffords in

particular, I have every expectation that this committee will indeed craft a bipartisan, common sense bill that the entire Congress can support.

I would like to thank all of our witnesses for taking time to be with us today. I look forward to their testimony.

Thank you.

The CHAIRMAN. Thank you both. We have taken a great deal of your time, but that emphasizes the importance of this issue. We will continue to consult and work with both of you as we move forward.

Thank you both.

We will now turn to our second panel and Mr. John J. Bentivoglio. We are pleased to have you here.

You have someone with you, I believe.

STATEMENT OF JOHN T. BENTIVOGLIO, SPECIAL COUNSEL FOR HEALTH CARE FRAUD, OFFICE OF DEPUTY ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, DC, ACCOMPANIED BY LYNNE A. HUNT, CHIEF, FINANCIAL CRIMES SECTION, FEDERAL BUREAU OF INVESTIGATION

Mr. BENTIVOGLIO. I do, Mr. Chairman. This is Lynne Hunt, and she is chief of the Financial Crimes Section at the Federal Bureau of Investigation.

Good morning, Mr. Chairman and other members of the committee. My name is John Bentivoglio. I am special counsel for health care fraud for the Department of Justice. I am also the Department's chief privacy officer. I appreciate this opportunity to present the Department's views on the issue of medical records privacy.

The Department supports the enactment of Federal legislation to protect the confidentiality of patient health information. We recognize that patient medical records contain sensitive personal information, including past and present medical conditions, family medical history, prescription drug usage, and similar information. And we are aware of the studies and reports on the misuse of confidential information by employers, insurance companies and other private sector entities.

Accordingly, the Department supports the recommendations in the September 1997 report by the Secretary of Health and Human Services which outlines a comprehensive framework for Federal medical records privacy standards, including guidelines to ensure the security of identifiable health information, Federal safeguards and consumer controls of information in medical records, and holding health care entities responsible for employees who misuse protected information.

In addition, we support the recommendations in the Secretary's report that call for strong sanctions for violations of patient confidentiality, including criminal penalties for knowing and intentional violations of Federal medical records privacy laws.

At the same time, we urge you to recognize and accommodate the needs of law enforcement to investigate and prosecute civil and criminal violations and to protect public safety. In many cases, our ability to investigate and solve serious crimes, including violent crime, health care fraud and other serious offenses, turns on our ability to obtain individually identifiable health information in a

timely and appropriate manner. We are able to do so under current law, and we have used such authority in a responsible manner.

Moreover, law enforcement agencies have a strong incentive not to disclose investigate information, including confidential health information, beyond those with a need to know for a legitimate law enforcement purpose.

I would like to provide a couple of examples that demonstrate why law enforcement needs access, and access in a timely manner. During the course of a rape in Washington, DC, the victim slams a car door on the assailant's hand, possibly causing serious injury. Local police immediately contact emergency rooms in Washington, DC, Maryland and Virginia to determine if anyone matching the assailant's description has been treated for a serious hand injury.

A law enforcement agency conducts a comprehensive review of patient medical charts during an investigation of a hospital suspected of billing health insurance plans for services that were never rendered. During this lawful review, investigators discover notations in a medical chart that the patient has been physically assaulting other patients, causing serious physical injury. Hospital executives decide not to report these incidents to authorities in order to cover up inadequate staff coverage during the time of the assaults.

Finally, a person who has recently been released from a psychiatric facility barricades himself inside the offices of his former employer, kills two people and holds several more hostage. Negotiators need immediate access to his medical record to understand the kidnapper's diagnosis, discover what medications he may be taking, contact his psychiatrist, and to assist in resolving the situation without further loss of life.

These are just some examples where individually identifiable health information is disclosed to and used by law enforcement in an appropriate manner. In some cases, the need for health information is limited but urgent. For example, in the rape scenario described above, police are not seeking the entire medical file of the patient; rather, they simply need to know if a person matching the assailant's description has been treated for a serious hand injury. However, even though they are not in "hot pursuit" of a suspect, they need immediate access to that information.

In other cases, such as in a Medicare billing fraud, investigators will need access to hundreds of patient medical records, generally through an administrative or grand jury subpoena or civil investigative demand. In this scenario, it would be extremely burdensome and in some cases impossible to provide each patient with advance notice and an opportunity to be heard before the subpoena is enforced. Furthermore, notice to patients will unfairly and publicly broadcast law enforcement suspicion of a provider before any charges have been brought. Also, providers who receive premature notice that they are under investigation have the opportunity to destroy or conceal assets that might be seized in the future.

Law enforcement has an excellent track record in obtaining and using health information in an appropriate manner and in protecting its confidentiality. We are not aware of any systemic or widespread misuse of confidential health information by law enforcement, and Federal, State and local agencies are already under a

wide array of constitutional, statutory and regulatory requirements that protect the confidentiality of health information and ensure that it is obtained and used only for official law enforcement activities.

Given the frequent and sometimes urgent need for law enforcement access to this information, the Department recommends that we maintain current Federal privacy protections. We urge the committee to follow the September 1997 report of the Secretary of Health and Human Services which recommends that law enforcement agencies be protected from new restrictions and provided no additional authority for access to medical records.

As the committee moves forward, we would appreciate the opportunity to work with the committee on the development of patient privacy legislation.

Again I appreciate the opportunity to present the Department's views and look forward to answering your questions.

Thank you.

[The prepared statement of Mr. Bentivoglio follows:]

PREPARED STATEMENT OF MR. BENTIVOGLIO

Good morning. I am John Bentivoglio, Special Counsel for Health Care Fraud in the Office of the Deputy Attorney General. I also serve as the Department's Chief Privacy Officer. I appreciate this opportunity to present the Department's views on medical records privacy legislation.

The Department supports the enactment of federal legislation to protect the confidentiality of patient health information. We recognize that patient medical records contain sensitive personal information, including past and present medical conditions, family medical history, prescription drugs, and similar information. And we are aware of the studies and reports on the misuse of confidential health information by employers, insurance companies, and private-sector entities. Accordingly, the Department supports the recommendations in the September 1997 report by the Secretary of Health and Human Services,, which outlined a comprehensive framework for federal medical records privacy standards, including guidelines to ensure the security of identifiable health information, federal safeguards and consumer controls of information in medical records, and holding health care entities responsible for employees who misuse protected information. [1]

In addition, we support the recommendations in the Secretary's report that call for strong sanctions for violations of patient confidentiality, including criminal penalties for knowing and intentional violations of federal medical records privacy laws.

At the same time, we urge you to recognize and accommodate the needs of the law enforcement community to investigate and prosecute civil and criminal offenses and to protect public safety. In many cases, our ability to investigate and prosecute serious crimes—including violent crime, health care fraud, and other offenses—turns on our ability to obtain individually identifiable health information in a timely and appropriate manner. We are able to do so under current law and we have used such authority in a responsible manner. Moreover, law enforcement agencies have a strong incentive not to disclose investigative information, including confidential health information, beyond those with a need to know for legitimate law enforcement purposes.

The following examples, however, provide compelling evidence of situations where law enforcement needs access to such records:

• During the course of a rape in Washington, DC., the victim slams a car door on the assailant's hand, possibly causing serious injuries. Local police immediately contact emergency rooms in Washington, D.C., Maryland and Virginia to determine if anyone matching the assailant's description has been treated for a serious injury.

• A law enforcement agency conducts a comprehensive review of patient medical charts during an investigation of a hospital suspected of billing health insurance plans for services that were never provided. During this lawful review, investigators discover notations in one medical chart that the patient has been physically assault-

[1] "Confidentiality of individually-identifiable health information," recommendations of the Secretary of Health and Human Services, pursuant to section 264 of the Health Insurance Portability and Accountability Act (September 1997).

ing other patients causing serious physical injury. Hospital executives decide not to report these incidents to authorities in order to cover up inadequate staff coverage during the time of the assaults.

• A person who recently has been released from a psychiatric facility barricades himself inside the offices of his former employer, kills two people, and holds several more hostage. Negotiators need immediate access to his medical record to understand the kidnapper's diagnosis, discover what medications he may be taking, contact his psychiatrist, and to assist in resolving the situation without further loss of life.

These are just some examples where individually identifiable health information is disclosed to, and used by, law enforcement in a lawful and appropriate manner. In some cases, the need for health information is limited but urgent For example, in the rape scenario described above, police are not seeking the entire medical file of a patient—rather, they simply need to know if a person matching the assailant's description has been treated for a hand injury within the past 24 hours. However, even though they are not in "hot pursuit" of a suspect they need immediate access to such information.

In other cases, such as in a Medicare billing fraud, investigators will need access to hundreds of patient medical records, generally through an administrative or grand jury subpoena, or a civil investigative demand. In this scenario, it would be extremely burdensome, and in some cases impossible, to provide each patient with advance notice and an opportunity to be heard before the subpoena is enforced. Furthermore, notice to patients will unfairly and publicly broadcast law enforcement suspicion of a provider before any charges have been brought. Also, providers who receive premature notice that they are under investigation have the opportunity to destroy evidence or conceal assets that might be seized in the future.

Law enforcement has an excellent track record in obtaining and using health information in an appropriate manner and in protecting its confidentiality. We are not aware of any systemic or widespread misuse of confidential health information by law enforcement. Federal, state and local law enforcement agencies arc already subject to a wide array of constitutional statutory, regulatory and administrative requirements that protect the confidentiality of health information and insure that it is obtained and used only for official. law enforcement activities. At the federal level, access to medical records generally is obtained through administrative or grand jury subpoenas or search wan-ants. Grand jury proceedings are governed by strict secrecy rules. Search warrants must be approved by a neutral magistrate and supported by probable cause. Many agencies have internal rules and regulations governing access to, and disclosure of investigative information, including health information. Law enforcement prosecutors are bound by ethical proscriptions not to improperly obtain and use evidence. Finally, as a practical matter, law enforcement has a strong interest in not publicly disclosing the fruits of an on-going investigation.

The Department of Justice has taken a number of internal steps to safeguard the privacy of confidential health information consistent with our law enforcement responsibilities. Since health care fraud investigations frequently require access to patient medical information, the joint DOJ-HHS guidelines implementing the Health Insurance Portability and Accountability Act of 1996 (HIPAA) include detailed guidance on access to, and use of individually identifiable health information[2] In October 1998, the Deputy Attorney General issued a memorandum to all DOJ personnel reiterating the importance of protecting the confidentiality of medical records, reaffirming the privacy safeguards in the HIPAA guidelines, and describing additional steps DOJ personnel should take to safeguard confidential health information. Health records confidentiality is a recurring subject covered in training of Department health care attorneys and investigative agencies. The Department is in the process of developing even more specific guidance governing the disclosure, use and handling of health information.

Given the frequent and sometimes urgent need for law enforcement access to health information, the Department recommends that we maintain current federal and state privacy protections. Any new restrictions would seriously impair law enforcement's ability to combat violent crime, health care fraud, and other illegal activities. Consistent with this position, we do not believe that any new authority is necessary. We urge the Committee to follow the September 1997 report of the Secretary of Health and Services, which recommends that law enforcement agencies be protected from new restrictions and be provided no additional authority to access medical records. As the Committee moves forward, we would appreciate the oppor-

[2] "Guidelines Implementing the "Health Care Fraud and Abuse Control Program, Section VI; Confidentiality Procedures: Provision and Use of Information and Data," (January 24, 1997)

tunity to work with the Committee on the development of patient privacy legislation.

Again, I appreciate the opportunity to present the Department's views on these issues and look forward to answering any questions you might have. Thank you.

The CHAIRMAN. Thank you very much.

You testified that "Federal, State, and local law enforcement agencies are already subject to a wide array of constitutional, statutory, regulatory, and administrative requirements that protect the confidentiality of health information." How do you respond to those who argue that these protections do not guarantee privacy and that stricter hurdles are needed for law enforcement?

Mr. BENTIVOGLIO. In general, we do take advantage of constitutional and statutory processes for obtaining medical records. Typically, at the Federal level, we get this through the grand jury subpoena process or through a search warrant.

But the examples that I described demonstrate that in some situations going through that process would be unduly burdensome and could jeopardize public safety. In those instances, I think we look to the very sound track record of law enforcement, which does not include really widespread or systemic misuse of confidential health information, and I think that is largely because we have such a strong incentive to use the information in an appropriate manner and not to publicly disclose it beyond the needs of a law enforcement investigation.

The CHAIRMAN. You mentioned that the Department is in the process of developing more specific guidance governing the disclosure, use, and handling of health information. When do you expect the guidance to be available for members of this committee?

Mr. BENTIVOGLIO. I cannot give you a specific deadline. I would think that in the next several weeks or months, we should be able to issue that. That guidance will direct our personnel to do things like redact documents that are disclosed in an administrative or a judicial proceeding, to ensure that we have appropriate security of confidential medical records and the like. We would be happy to share that with the committee as soon as it is available.

The CHAIRMAN. Ms. Hunt, do you have any comments to add?

Ms. HUNT. Yes, just very briefly, thank you.

Good morning. As Mr. Bentivoglio stated, I am Lynn Hunt, chief of the Financial Crimes Section of the Federal Bureau of Investigation.

I want to thank the chairman and the entire committee for allowing me to appear this morning to express not only FBI's but I believe all of law enforcement's concern with proposed medical records legislation which could severely hamper law enforcement's efforts to address a host of crime problems plaguing the American society.

In 1996, Congress enacted comprehensive legislation to combat the health care fraud crime problem, which continues to rob Americans of billions of dollars annually and affects the quality of medical care that we all require.

The Health Insurance Portability and Accountability Act of 1996 gave the FBI increased funding and new legal tools to address this very crime problem. We at the FBI interpreted this as a message that Congress wanted the FBI to step up our efforts. We responded.

I and other senior management officials have used this increased funding to hire, equip and train more agents to be assigned to health care fraud crime matters. The Bureau now has the equivalent of 420 agents investigating over 2,800 cases of health care fraud—a more than threefold increase from the early 1990's. This is a serious commitment of investigative resources.

Let me assure you that these 2,800 investigations do not involve instances of honest billing mistakes, as we have neither the resources nor the desire to pursue these matters. There are other remedies to correct these mistakes that do not require an investigation by the FBI.

What our agents are pursuing are criminals who commit massive fraud and who may put financial gain over the care and medical needs of the patients.

My staff and I have reviewed a number of bills introduced as well as proposed, and we have grave concerns about the new burdens and restrictions that many will place on law enforcement, particularly in our health care fraud enforcement efforts. It is our most basic need to be able to compare what was billed to Government-sponsored as well as private health care plans with what services were actually provided to the patient.

The FBI has investigated literally thousands of allegations of egregious fraud in this area, and I am not personally aware of any instance in which our agents have been careless with personally identifiable health care information. In fact, we take great steps to prevent this very occurrence.

The FBI and the entire Department of Justice agree that new protections are needed for patient records. However, absent documentation of any systemic abuse by law enforcement, we would urge Congress that no new legislation be enacted that would unduly burden law enforcement in investigating serious criminal conduct as well as civil fraud.

Mr. Bentivoglio indicated that these restrictions would adversely impact on many other area of law enforcement to include serious violent crimes, hostage situations and terrorist activities. What about those States that currently have laws requiring the mandatory reporting of gunshot wounds? Furthermore, how would the requirement contained in these bills impact on the excellent working relationship that presently exists between the investigators and prosecutors of the Department of Justice and the Health Care Financing Administration, as well as the special investigative units of private insurance companies?

What about qui tam relaters and other good citizens who want to report health care fraud to the FBI or other law enforcement agencies? Would they be committing a criminal act by furnishing documentary evidence to law enforcement?

These are some of the issues which we urge Congress to consider. As Mr. Bentivoglio pointed out, the Department views with enormous concern the right of Americans to have their medical records protected from unwarranted disclosure. He mentioned that the Deputy Attorney General recently issued a memorandum stressing the need to protect individually identifiable health information obtained during the course of our investigations and prosecutions. This memorandum was forwarded to all FBI field offices so that

they too would be reminded of the importance of confidentiality. I believe that this should be reinforced at the FBI Academy so that all new agents are clear on this issue, and I will personally guarantee this committee that this will be done.

In conclusion, I urge you not to recommend new restrictions on law enforcement access when you consider medical records privacy legislation.

Thank you.

The CHAIRMAN. Thank you.

I would remind you that we have to get this out and moving; we hope to have it marked up and out of this committee by the end of May. So I would hope you would keep in touch with us, and we will keep in touch with you to make sure we end up with a product that you will not feel unduly burdensome.

Mr. BENTIVOGLIO. We would be happy to work with the committee, Mr. Chairman.

The CHAIRMAN. Senator Dodd.

Senator DODD. Thank you, Mr. Chairman.

Let me just get very practical with you. In your testimony, you cited an example of a rape case in which there were some wounds or some blood samples of the alleged perpetrator, and you needed to access that information.

I wonder if you could just take that example, a very concrete example, and explain how law enforcement currently accesses those record, number one, and how specifically would the bills that have been introduced impact, in your view, the present process. Take us through what you would do right now, very briefly, in that kind of absolute and clear fact situation.

Mr. BENTIVOGLIO. Well, that offense would be a violation of State law, so if it happened in Washington, DC, the DC police would probably go to the local emergency rooms and see if someone had been treated for a hand injury that matched the assailant's description. If that were the case, they would probably go back and get a search warrant in that situation.

Senator DODD. That is under the present situation.

Mr. BENTIVOGLIO. Correct.

Senator DODD. All right.

Mr. BENTIVOGLIO. The difficulty that we have with the legislative proposals is that even that initial contact with the emergency room would be problematic because they could not disclose that information to us, so we could not even get a search warrant of the hospital——

Senator DODD. Under which bill? Which bill are you talking about now?

Mr. BENTIVOGLIO. Under virtually all the bills; under the bill introduced by the chairman, Mr. Bennett, and Mr. Leahy as well.

Senator DODD. The chairman's bill as well?

Mr. BENTIVOGLIO. Yes, sir.

That highlights a dilemma that we face. In that situation, that initial contact with the emergency room, we are not asking for the patient's entire medical file. We are asking merely whether a person has been treated for an injury. And in that sense, we do not think that the grand jury process or the search warrant process is practical. Since it is a local investigation, they would have to go to

local courts in Montgomery County, Price George's Country, the District, Arlington, and Alexandria to get a search warrant, and without the initial information about whether a patient who matches the description has been treated for that type of injury, they could not even get any compulsory process.

Senator DODD. Well, the ACLU disputes these alarms, as you might not be surprised, and I guess we are going to hear from them, Mr. Chairman. I appreciate that. Thank you.

The CHAIRMAN. Thank you, Senator Dodd.

Senator Hutchinson.

Senator HUTCHINSON. Thank you, Mr. Chairman.

Let me just follow up on what Senator Dodd said. You stated that you thought no new restrictions should be added. Exactly what are you required to access medical records currently—individually identifiable medical records.

Mr. BENTIVOGLIO. Well, if we were to obtain the records under a grand jury subpoena, there are standards for when we could issue a grand jury subpoena for those records. It has to be relevant to an ongoing criminal information. If we wanted a search warrant, we would have to go to a magistrate based on probable cause to get certain records.

In the instance of the rape example that we were discussing, there would not be any restrictions currently on our going to a hospital and asking if someone matching this description has been treated for a hand injury.

Senator HUTCHINSON. OK. In that instance, I think you said that you went to the hospital emergency room, and you asked, an then you would go back and get a search warrant, but you said "we might want to go and get a search warrant." Would you be required to get a search warrant, or could you demand access to their records currently?

Mr. BENTIVOGLIO. We could probably ask them for those records. Most hospitals would not provide them, and I think that in the vast majority of cases, we would go back and get a search warrant as a matter of good law enforcement practice, because in that situation, we would be looking for the entire patient record.

Senator HUTCHINSON. But there are currently no requires that you do that.

Mr. BENTIVOGLIO. Correct.

Senator HUTCHINSON. When Senator Leahy was here, he gave the example of video records. If you wanted to get someone's video rental records, what would you currently have to do?

Mr. BENTIVOGLIO. You would need to get a court order. I would like to address that issue.

Senator HUTCHINSON. I want you to have that opportunity.

Mr. BENTIVOGLIO. Thank you, Senator.

Video record are rarely needed for any type of investigation, whether it is a violent crime, health care fraud or the like, so those restrictions which are very severe do not get in the way of many investigations that we face. If those same restrictions were put in place on health care information, it would have a devastating impact on our ability to solve some crimes.

Senator HUTCHINSON. So the requirements, as I understand it, in the various bills are fairly consistent—that the information would

need to be relevant, material to ongoing investigations; the investigative needs of the agency could not be reasonably satisfied with de-identified health information; the law enforcement need for information outweighed the privacy interests of the individual involved.

Explain to me—is it simply a matter that the time required to demonstrate those requirements would make it unwieldy or interfere, then, with good law enforcement? Those sound fairly reasonable, that that should be demonstrable before you have access to that information.

Mr. BENTIVOGLIO. Yes, Senator. If it were only those requirements, we would be less troubled, but those requirements are coupled with the need to go to a court and get an order before we get access to this kind of information, and that is the burden that would be troubling to us. If we had to go and get a court order before, for example, going to a hospital, that would be very burdensome, particularly in the example I described where you would have to go to multiple jurisdictions.

Senator HUTCHINSON. Are you required to get a court order in certain instances today? You have mentioned video rental records, but it was my impression that getting a court order was fairly routine, that it was frequently done, that it was not something that required a lot of time.

Mr. BENTIVOGLIO. Well, a search warrant does take—you have to prepare an affidavit, you have to go to a court and get that order, and you need probable cause to establish that the evidence you will seize will be relevant to a crime.

In the rape example that I described, we would not even know, going to a hospital in the first instance, whether a person meeting that description had been treated for the type of injury that we are looking for, so we would not even have probable cause to go to a court and say we want the patient records from Hospital "X". That is why we need the ability to contact those local hospitals, get that preliminary information, determine whether there is probable cause, and then go back and get a court order.

Senator HUTCHINSON. I think you touched on this, but could you expand on how the various proposals would impact current mandatory reporting requirements? We have had prosecutors who have called us, concerned about mandatory requirements for reporting gunshot wounds, knife wounds. How do you see these proposals impacting current laws?

Mr. BENTIVOGLIO. In our review of the legislation, I think that both the Bennett and Leahy bills would preempt the mandatory reporting laws—laws, for example, on mandatory reporting of gunshot wounds. The bill introduced by the chairman has an explicit exception for that, so that reporting under Federal or State law could continue to occur.

Senator HUTCHINSON. I appreciate your answers. They have been very responsive. I think that clearly, the need for a balance in the bill that the committee puts forward is essential, and I appreciate the chairman's willingness to work with you and the Department.

Senator DODD. Tim, would you just yield on one point?The Senator asked you a question about how burdensome. Specifically, watt do you do? How burdensome is this, really?

Mr. BENTIVOGLIO. To get a search warrant?

Senator DODD. Yes.

Senator HUTCHINSON. I will be glad to yield.

Senator DODD. Why don't you go through how burdensome that is? I mean, the police department is showing up at a hospital——

Mr. BENTIVOGLIO. Most hospitals would not just simply turn over a patient's records.

Senator DODD. Right. So now you have got to go back. How much time does that take? Is it an hour, a day, a week?

Mr. BENTIVOGLIO. At least several hours or longer. You would need an affidavit from an agent describing the probable cause. That would need to be submitted to a court, and the court would need to rule on that. And when you are making that type of statement under oath, you need to be sure that all your facts are straight, and it is very serious to seek a search warrant from a court.

Senator DODD. But it should be—shouldn't it be serious?

Mr. BENTIVOGLIO. Absolutely, Senator.

Senator DODD. Thank you for yielding.

The CHAIRMAN. Any final comments, Senator Hutchinson?

Senator HUTCHINSON. I recognize the need for a balance, but I think that if we are talking about an inconvenience, not something that is going to dramatically hamper law enforcement's efforts, we need to lean to the side of the protection of the individual.

So as we work through this, I hope we will keep that in mind, and the clarification that we are talking in terms of possibly a few hours as opposed to something that is going to be a very, very length process, we need to keep in mind.

Mr. BENTIVOGLIO. Senator, if I might respond to that, the difficulty in the example we described, though, is that we could not go to a court and get a search warrant if we did not have some idea that that assailant was treated at a particular hospital. If we could not make that initial contact with the local hospitals to determine if someone meeting a certain description has had a certain type of injury treated, we could not get a search warrant in that instance. So I would argue that it is not a matter of an inconvenience; in some situations, if we do not have access to that initial information, we cannot move forward. And a search warrant or grand jury subpoena would not be available to us.

Senator HUTCHINSON. So currently, if you go into a hospital and ask, "Did you treat someone with this wound?" they will automatically give you the answer?

Mr. BENTIVOGLIO. In many instances, they would, yes.

Senator HUTCHINSON. Thank you, Mr. Chairman.

The CHAIRMAN. Senator Wellstone.

Senator WELLSTONE. Thank you, Mr. Chairman.

I think this is an extension of the question that Senator Hutchinson and Senator Dodd were asking. As a Federal prosecutor, can you give us some examples or an instance in which law enforcement has sought a court order for medical records and actually been denied, and where the denial then thwarted your being able to be successful in your investigation?

Mr. BENTIVOGLIO. I cannot think of any specific examples. We do not keep track of instances where we have not been able to pursue

matters for one reason or another, so I cannot provide you with any specific examples.

Senator WELLSTONE. I think that is part of the question that we are trying to get at here. The reason I mention this is that I do think that part of what you are suggesting—although I fully appreciate your framework—breaks precedent with privacy laws that would allow law enforcement to gain access to very sensitive personal information without some legal process. So I think the question of whether there is some evidence that you can point to where you sought a court order for medical records and you were denied—maybe you could supply us with that information, because for me, that is a key point.

Ms. HUNT. The only thing I can come up with that is fairly close is that we had a situation where we requested a court order for medical records, and the judge was very nervous about the privacy issues associated with giving medical records. He took it under advisement for several weeks. When he then gave us the ability to get the records, he only gave us the records without the identifying information, which then turned out to be useless for us because we could not compare the billing records with the medical records, which is what we usually need to do in these health care fraud cases.

The judge was nervous, and as a result, even though we got the records, they were useless.

Senator WELLSTONE. What is the burden for getting a court order?

Mr. BENTIVOGLIO. It depends on what type of order you get. For example, for a search warrant, you need probable cause to establish that the persons or places to be seized or searched are going to yield evidence of a crime. So essentially, you need probable cause.

Senator WELLSTONE. I do a fair amount of work on tough issues dealing with substance abuse. In the course of a fraud and abuse investigation of a substance abuse clinic, what happens if DOJ uncovers evidence of illegal drug use on the part of a patient—can that information be used to prosecute the patient? Do you follow my question?

Mr. BENTIVOGLIO. There are already heightened privacy protections for substance abuse records under Federal law. So that typically, to get the information in the first place, we would need a court order because of concerns about the unique nature of substance abuse records. So we would need a court order.

Senator WELLSTONE. So in the absence of that, the answer would be no?

Mr. BENTIVOGLIO. Yes.

Senator WELLSTONE. I was just told—I do not want to pretend that this is my own view—that right now, this is only for federally-funded treatment. Is that the only protection there is with the court order—or do you know?

Mr. BENTIVOGLIO. I believe that that is the case.

Senator WELLSTONE. I am told—I am not a lawyer—I will ask my staff to pose the question.

Ms. REST-MINCBERG. I understand it is very arcane, and like many privacy issues, tucked into various pieces of legislation, there

are different protections for medical records. But I believe the extra protection that you are referring to for people who are in substance abuse treatment only extends to people who are in a program that has Federal funding and their treatment is federally-funded. I see some people nodding their heads back there.

Mr. BENTIVOGLIO. I believe that that is right, and I think we can make sure that we get that answer to you for the record.

Ms. REST-MINCBERG. OK.

[Information follows:]

[The information from the Department of Justice was not received at press time. If and when received will be retained in the files of the committee.]

Senator WELLSTONE. That would be good. I am glad I thought of that question. [Laughter.]

Thank you, Mr. Chairman.

The CHAIRMAN. Senator Frist.

Senator FRIST. Thank you, Mr. Chairman.

The fundamental question is what do you do in terms of search warrants that is specific for health care, and are there specific procedures. Let me set the background for this. Recently, I was back in Tennessee and was made aware of a situation which I have numerous articles about and which both of you probably know something about. Let me just share with you what I was told.

On February 24, 1999, approximately 37 Federal and State agents with guns and bulletproof vests executed a search warrant on Woods Memorial Hospital, a nonprofit, 72-bed hospital which operates a home health agency and nursing home, all of which are owned by McMinn County, the county hospital. Agencies represented by these individuals included the Office of Inspector General, the Federal Bureau of Investigation, and the Tennessee Bureau of Investigation.

I was told that the unprofessional conduct of many of the agents upset families, patients and workers, and in some cases jeopardized patient safety. So I am coming to health care facilities and raids or search warrants.

This is referenced by the president of the Tennessee Hospital Association, who basically says, quoting from the letter, that "I believe the agents participating in the Woods Memorial Hospital raid far exceeded the boundaries of the search warrant. In short, the Department of Justice in its endeavors to ferret out fraud and abuse should not be allowed to put patients' health at risk or frighten, intimidate and humiliate innocent nurses and others with heavy-handed and inappropriate investigative tactics."

That is from the letter. There are numerous articles. In an editorial from the local paper in a small town, Athens, TN, The Daily Post Athenian—Ooltewah is right next to that—and again, there are numerous articles, but I will quote—"Dozens of these Federal agents descended upon the hospital wearing handguns and bulletproof vests—a scary sight in itself. They flashed their badges and demanded to know who people were and watt they were doing at the hospitals. These agents, with an air of arrogance about them, herded employees into offices and began questioning them without any explanation of why they were being interrogated. It was a frightening experience for all of the employees, who found them-

selves feeling as if they were at the mercy of the Federal agents. Some of the hospital workers even feared for their own safety."

"And it was not just the employees"—and this is what bothers me the most, personally—"And it was not just the employees who found themselves recoiling in fear from the Federal agents. Patients and visitors alike were treated with total disregard and were given no respect by the agents."

"We found it especially troubling to learn that these Federal employees burst into the dialysis center where patients with extremely fragile conditions were being treated and started acting like a schoolyard bully."

I had the hospital administrator come in recently—these are all constituents of mine—and basically describe what happened as agents with a search warrant came into a dialysis center where patients were actively being treated. It is interesting that one of the patients in that dialysis center when the agents came in had hepatitis C, which as you know is a very infectious agent, and the description—and this was all documented in numerous letters—is frightening to someone like myself and made me ask, regardless of whether the hospital has done something or not, what assurances we can give patients and doctors and nurses who are in these hospitals when a search warrant—and all of these bills say you can have search warrants for medical records—first of all, just the behavior. The description of the narrative of what happened: "Employees were forced into a small office in the dialysis center. Between 10 and 12 people were crammed into a 10-by-12-foot office which also contained bookcases. One nurse was claustrophobic and nearly fainted due to the tight space; she started yelling, and they finally let her out." The description goes on: "Agents also raided the dialysis center next door. The director of the center was washing artificial kidneys in a back room when an agent walked in with his hand on his gun and loudly demanded to know his name and why he was there. The agents intimidated the patients and staff of the dialysis center and home health department and disturbed dialysis patients who were in a fragile State due to their disease. They trampled through sterile areas. They did not wear any protective clothing or gloves in these areas to guard against infecting the patients, who had open blood lines."

Staff were not allowed to use the telephone. "In a home health care agency where there were ongoing calls coming in from people who needed help, they were not allowed to use their telephones. Employees had to raise their hands. Some personal items were taken."

When I read this, it makes me think—and now that there have been enough people who have come through my office from this county-owned hospitals—and it disturbs me a little bit, and I want to make sure in all of the legislation that we have some recognition that health care facilities, when there are raids or you are taking medical records even with a search warrant, are protected. And my question is: Is there anything specific in terms of the regulations that recognizes that delivery of health care is in an environment that is very different than where other types of raids would be carried out?

Mr. BENTIVOGLIO. Indirectly, yes. I do not want to say that there are specific guidelines on search warrants executed at hospitals. I should say that as a matter of general practice, our people know not to disrupt the ongoing operations of the health care facility when executing a search warrant or a subpoena. Where possible, we will try to serve it, for example, at night, when there are not patients around. We will try to do so in a manner that disrupts the facility as little as possible.

In that particular instance, Senator—I have seen those press clips as well, and I have asked for a report on what occurred in that situation—and at least from the information I am getting, many of those facts are grossly distorted. Nonetheless it is very serious when we execute a search warrant during the day in a hospital facility, and we are still looking at that to see if we did something wrong, and if we did not, watt procedures we should have in place to make sure that we are sensitive.

There is no doubt that we have tools available to us that need to be used responsibly even in the absence of legislation. We need to do a good job with those tools and have people confident that when you give us the tools to fight health care fraud or violent crime or terrorism, they are being used appropriately. So putting aside legislation, we need to make sure that we are getting it right.

Beyond that, I do not want to comment on that particular matter because it is an ongoing investigation, but we should be able to provide our side of the story on that to the committee so that you are not left with the impression that the facts are reported in the press were completely accurate.

Senator FRIST. Thank you.

The CHAIRMAN. Yes, I would appreciate that, because I would like to know what action is taken if it is felt that this was not appropriate conduct.

Mr. BENTIVOGLIO. Yes, Mr. Chairman.

The CHAIRMAN. Senator Reed.

Senator REED. Thank you, Mr. Chairman, and I want to thank the witnesses for their testimony.

In response to Senator Dodd's question, you seemed to imply that all of the legislation would unduly restrict law enforcement activities, and you cited in your testimony some specific examples which on the surface appeared very compelling. You argue, for example, that legislation should not stop the police from checking out emergency rooms if a criminal might be seeking treatment. But I would note—and I am not a cosponsor—that Senator Leahy's and Senator Kennedy's bill at section 208(i) does in fact have a "hot pursuit" exception which I think could reasonably fit your rape example, since I presume that would be "hot pursuit." The police get a report of an incident, they immediately go to the emergency room and ask for a report of anyone who has appeared or will appear in the next reasonable amount of days, hours, whatever.

In addition, there is a section 204(b) which has a "Harm to Others" provision which would be that if someone is going to cause harm to others, you can get their records, which would cover your example of psychiatric discharge holding people hostage. And then, at section 207, there is a provision in a noncriminal context for

oversight of records and disclosing these records with a balancing test.

The point is that I think there is legislation which is trying to address those issues, and by way of allowing you a comment, my comment would be that it seems to me unhelpful for the Department of Justice to come here and simply say Congress cannot do anything—do not do anything. Technology alone is changing the calculations, and to simply sit there and say you cannot do anything because it will impair or impact on the law enforcement, I think is avoiding an issue which we have to deal with in a principled way. And again, I am not a cosponsor, but I think that the Leahy-Kennedy bill, and I would assume the Dodd-Jeffords bill, are trying to deal with these issues. So could you comment on that and perhaps be a little more helpful?

Mr. BENTIVOGLIO. Yes, Senator. First, we do recognize that the bills try to strike the right balance between law enforcement and privacy interests. We would like them to go a little further in the law enforcement area to address specific needs.

The "hot pursuit" example is a good one. Under case law which defines "hot pursuit," I believe that that rape example would not qualify as "hot pursuit." We do not have a specific suspect in mind. We do not know where they are. We may have a general description and an injury that they might have. But I would think that under the definition of "hot pursuit" in the case law, we could not go to a hospital under that circumstance and get that information.

I also do not want to leave the impression that we think all the provisions in the bills are bad. There are some that we could live with—for example, the requirement of destruction of records after we obtain them. That seems to make good sense. It would impose a burden, but we would think that that is reasonable. Provisions dealing with the redaction of records that we disclose in the course of a judicial proceeding or the like also seem reasonable—a burden, yes, but a reasonable burden given our needs.

But it is that initial access to information, and not necessarily the entire patient file, but information nonetheless that would qualify as individually identifiable health information, that give us great pause, and we would be happy to work with the committee to see if there is an appropriate balance that could be struck in that area.

Senator REED. I think that would be the approach. I would also point out that I believe that this "hot pursuit" in particular is being criticized by some—the ACLU and others—as going too far. But what I find unhelpful is the notion of rather than coming forward and giving us specific advice with respect to, for example, the "hot pursuit," situation you simply reject all efforts of redress. Maybe "hot pursuit" is the wrong choice of terminology. Maybe, rather than "hot pursuit," it is "in the immediate investigation of a crime to ascertain the identity and not the medical"—if that is what you need, those kinds of helpful, specific comments I think should be presented to the committee.

I thank the chairman.

The CHAIRMAN. Thank you, and I would agree with your statement.

Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Law enforcement officials need access to other kinds of personal records to investigate and prosecute cases. You have already said that it would be a rare case where you would need access to video store records, and we have talked about the amount of privacy afforded to those. But surely it would be very common for you to seek access to bank records. Could you tell us watt kinds of privacy protections apply when you try to access bank records?

Mr. BENTIVOGLIO. Under the Right to Finance Privacy Act, it does require some type of court order or subpoena for those types of records.

Senator COLLINS. So what you are arguing is that we should provide greater protection to bank records than we do health records. I just cannot accept that argument. Given the sensitive information that is contained in medical records, how can we justify providing less protection to the access of medical records than we do to bank records?

Mr. BENTIVOGLIO. Senator, I understand the logic of that comparison, and it seems compelling, but I could only say that the examples cited in my testimony demonstrate why in some situations, we need limited but urgent access to individually identifiable health information. That is a very concrete example of where a court order, either a search warrant or a grand jury subpoena, would be a serious burden.

Senator COLLINS. I just do not think getting a court order is a serious burden. But let me take one of the examples in your testimony because they are compelling examples; they are probably the best examples for allowing you immediate access without the kinds of protections that I think we would like to have.

Let us take the example—perhaps your most compelling example—of the rapist who has his hand slammed in the car door. What if on the same night, my friend Senator Hutchinson also slammed his hand in the car door and went to the hospital, or my friend Senator Reed was skiing and broke his hand and was in that same hospital. Under your scenario, you would have access to their records without any cause, without any reason to believe they had been involved in a crime.

I am troubled by that. I am troubled by that sweeping accessibility to sensitive records.

Mr. BENTIVOGLIO. Senator, I was trying to make clear and perhaps I did not that in that situation, what we would be looking for is whether someone has been treated for a particular type of injury. We would not go to the hospital and demand from the emergency room staff the entire patient file. If we wanted that patient file, we would go back and seek a search warrant or a subpoena for that file.

So I think the example demonstrates the accommodation and balancing that needs to occur. I agree that getting access to an entire patient file is very serious and that our access should be limited for that in some situations; but there are other situations where we need at least identifying and other types of information that is not as sensitive, and we need it on a very time-sensitive basis.

Senator COLLINS. But I think the legislation before us would give you access to that kind of information. I was very disappointed when, last September, Secretary Shalala came to us and proposed that there be essentially no new privacy protections applying to law enforcement in this area. I would strongly urge the administration to reconsider its approach, to adopt the advice of the Senator from Rhode Island and be more helpful to the committee in this area.

We do not want to interfere with the legitimate access to sensitive information if it is absolutely necessary for an investigation. I have done extensive work in the area of Medicare fraud. I realize that it is a very troubling problem, and I do not want to put unnecessary impediments in your way, but neither do I want to give you complete and unfettered access to the most sensitive information about individuals. And it seems to me that there is an answer here and that the legislation before us has tried very, very hard to strike the right balance.

So I would urge you to work with the committee as we go forward, because I frankly do not think you will find a great deal of sympathy for your position that there be no privacy protections at all.

Thank you, Mr. Chairman.

Mr. BENTIVOGLIO. Well, Senator, we will take the committee up on the offer to be constructive. We do want to be constructive in this area, and we do recognize that the committee has attempted to balance some of these issues. We think a little more work needs to be done, but your point is very well-taken, and we would like to come up and work with you.

Senator COLLINS. Thank you. We look forward to hearing your specific suggestions.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you both. As you can see, you perked a little interest here. We will be working very closely with you. This is a very important and sensitive area.

Mr. BENTIVOGLIO. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

We have 6 more witnesses and 3 panels, so I am going to try to expedite matters.

The third panel of witnesses today consists of representatives of the legal profession who will discuss the topic of law enforcement access. I am pleased to welcome Mr. Ronald Weich who will be testifying in behalf of the American Civil Liberties Union. Mr. Weich is a partner in the law firm of Zuckerman, Spaeder, Goldstein, Taylor & Kolker in Washington. He has previously served in a number of senior staff positions in the U.S. Senate, including general counsel to the Committee on Labor and Human Resources. Mr. Weich, we look forward to your testimony.

Also on panel 3, testifying in behalf of the American Bar Association, is Professor Robyn S. Shapiro, director of the Center for the Study of Bioethics, and professor of bioethics at the Medical College of Wisconsin. Professor Shapiro is also a partner in the health law practice group of Michael Best & Friedrich in Milwaukee. Professor, we are privileged to have the benefit of your expertise this morning.

Mr. Weich, please proceed.

STATEMENT OF RONALD H. WEICH, ZUCKERMAN, SPAEDER, GOLDSTEIN, TAYLOR & KOLKER, WASHINGTON, DC, ON BEHALF OF THE AMERICAN CIVIL LIBERTIES UNION; AND ROBYN S. SHAPIRO, DIRECTOR, CENTER FOR THE STUDY OF BIOETHICS, MEDICAL COLLEGE OF WISCONSIN, MILWAUKEE, WI, ON BEHALF OF THE AMERICAN BAR ASSOCIATION

Mr. WEICH. Thank you, Mr. Chairman, members of the committee. My name is Ronald Weich, and I am a partner in the law firm of Zuckerman, Spaeder, Goldstein, Taylor & Kolker, and a legislative consultant to the American Civil Liberties Union. I am pleased to appear before you today on behalf of the ACLU to discuss the issue of medical records confidentiality.

The ACLU is a nationwide, nonpartisan organization of nearly 300,000 members dedicated to protecting the principles of liberty, freedom and equality set forth in the Bill of Rights. For 80 years, the ACLU has worked to preserve and strengthen privacy in all aspects of American life.

Mr. Chairman, am I correct that my full written statement will be in the record?

The CHAIRMAN. That is correct.

Mr. WEICH. Then, I will summarize and focus my oral remarks specifically on the question of law enforcement access to an individual's medical records. And in discussing that issue, I would like to say that in addition to representing the ACLU, I bring two additional perspectives here.

First of all, I served as an assistant district attorney in New York City from 1983 to 1987; I prosecuted numerous criminal cases in which medical evidence was at issue, and I obtained search warrants, and I am prepared to talk about the process that that entails.

Second, from 1989 to 1997, I served as counsel to this committee and then to the Senate Judiciary Committee and participated in the formulation of health care and criminal justice policy during those years, and I think it is particularly relevant to my testimony today that I had an opportunity to work on mental health and substance abuse issues, two fields in which privacy of medical records is absolutely essential.

I am not going to reiterate the general points that have already been touched on about the importance of privacy in the medical records context because of the need for trust between doctor and patient. I would only note that those considerations are as important when you talk about law enforcement access to records as to any other kind of access. In other words, a patient is no more comforted hearing that the Government is reviewing his or her sensitive and intimate medical information than if they hear that a pharmaceutical company is. So the same policy considerations that lead the committee to want to have strong protections with respect to access to outsiders generally apply here.

We believe that it is very important that there be a principle embodied in Federal law which we believe is embodied especially in the Leahy-Kennedy bill, although, Mr. Chairman, I will very quickly say some good things about the Jeffords-Dodd bill as well. But with respect to Leahy-Kennedy, there is a principle that we want to emphasize, which is that Government agents should be required

to obtain judicial approval under a meaningful probable cause standard before they are granted access to medical records containing personally identifiable information.

There are two bills that we have analyzed. We have not had an opportunity to analyze Senator Bennett's bill because it was only introduced yesterday, although in general, that bill is similar to the chairman's bill. In some respect, it actually falls short of the privacy protections offered by the Jeffords-Dodd bill in the law enforcement area.

The Leahy-Kennedy bill is in our opinion the most protective of privacy in this area because it requires the police to obtain a court order or its functional equivalent before gaining access to records, and it sets a sufficiently high legal standard for such a court order. There has been a lot of discussion so far today about obtaining court orders and warrants on the one hand and subpoenas, and I think there is some confusion about the difference between those two processes.

A court order or a warrant requires judicial review. A subpoena, especially an administrative subpoena, or a summons, as the Jeffords-Dodd bill and I believe the Bennett bill also provide, are not judicially reviewed. A prosecutor, or indeed an FBI agent or a local law enforcement official, simply makes a demand of a hospital or another health care provider.

Under Leahy-Kennedy, that would not generally be permissible. Rather, a prosecutor would have to go before a judge to show that the information sought is relevant and material to an ongoing criminal investigation; the investigative needs of the agent cannot reasonably be satisfied by de-identified health information; and the law enforcement need for the information outweighs the privacy interests of the individual to whom the information pertains.

There is nothing magical about this. This is referenced to a 200-year-old principle embodied in our Constitution. Effectively, we are bringing the warrant requirement of the Fourth Amendment over to the medical records context. And there is a reason why it is not there now. If I happen to maintain my x-rays in my home because I have a bad knee, and I am going to take the x-rays from doctor to doctor, the police need a search warrant before they can seize the x-rays in a desk drawer in my home. But if the x-rays are in my doctor's office or in an insurance company computer or in an HMO's computer, I have lost my ownership, or at least current law does not recognize my ownership in those x-rays.

The bills that are before the committee would generally restore that ownership interest and would apply the kinds of Fourth Amendment protections here. And the Fourth Amendment simply embodies a balancing test between the interests of law enforcement—and we all recognize those important interests; nobody wants to be the victim of a crime, everybody wants vigilant law enforcement—on the one hand, and on the other hand, we have to recognize the value of privacy.

In my testimony, I review the specific ways in which we believe Kennedy-Leahy is superior to Jeffords-Dodd and two specific ways in which we think Jeffords-Dodd is superior to Kennedy-Leahy on the issue of law enforcement privacy.

I would say in conclusion, Mr. Chairman, that it is very important I feel as a former prosecutor that law enforcement be held to sensible rules. If the public believes—and Senator Frist's comments about the incident in Tennessee make this very clear—that law enforcement is overly zealous, too intrusive, playing outside the rules, there is a corrosive and destructive effect on the effectiveness of law enforcement, and that is dangerous to all of us.

Thank you.

The CHAIRMAN. Thank you, Mr. Weich.

[The prepared statement of Mr. Weich follows:]

PREPARED STATEMENT OF RONALD WEICH

Mr. Chairman and Members of the Committee: My name is Ronald Weich. I am a partner in the law firm of Zuckerman, Spaeder, Goldstein, Taylor & Kolker, and a legislative consultant to the American Civil Liberties Union (ACLU). I am pleased to appear before you today on behalf of the ACLU to discuss the issue of medical records confidentiality, and, more specifically, to address the question of law enforcement access to medical records.

The ACLU is a nationwide, non-partisan organization of nearly 300,000 members dedicated to protecting the principles of liberty, freedom and equality set forth in the Bill of Rights to the United States Constitution. For almost 80 years, the ACLU has sought to preserve and strengthen privacy in all aspects of American life.

In addition to representing the ACLU, I bring two additional perspectives to this hearing. First, I served as an Assistant District Attorney in New York City from 1983 to 1987 and prosecuted numerous criminal cases in which medical evidence was at issue. Second, from 1989 to 1997 I served as counsel to this Committee and then to the Senate Judiciary Committee, and participated in the development of federal criminal justice and health care policy during those years. Of particular relevance is my work for Senator Kennedy on mental health and substance abuse issues, two fields in which the confidentiality of medical records is essential.

My testimony is divided into three parts. The first section presents an overview of the ACLU's views on the privacy of medical records. The second section specifically addresses the circumstances under which law enforcement authorities should be granted access to an individual's medical records. The final section discusses other civil liberties implications of the medical records bills under consideration by the Committee.

I. OVERVIEW

Advances in technology have brought about a revolution in every aspect of health care, including the manner in which medical information is maintained and disseminated. Today, medical data can be collected, combined, collated, analyzed and distributed faster and easier than ever before. Huge quantities of health-related information can be stored electronically and transmitted across the country and around the globe with the click of a computer mouse. Much of this electronic activity benefits individual patients and facilitates public health efforts as well. But, like many technological advances, society's increased reliance on computerized medical records presents significant challenges to privacy.

Computer technology makes medical record keeping vastly more efficient. In the absence of legal safeguards, however, it also allows for virtually unlimited access to medical records without the knowledge or consent of the patient whose records are accessed. Health care providers and researchers are motivated to gather and share such information to improve the quality of care. But other entities may gather medical information for commercial and other non-medical purposes: pharmaceutical companies may want to solicit potential new customers, insurance companies may want to insure healthy policy holders and avoid unhealthy ones, employers may want to avoid hiring or keeping unhealthy employees on the payroll, and law enforcement agencies may be tempted to view computerized medical records as a vast new centralized data base to search for clues to crime.

Privacy is vital in the health care context because trust is a fundamental component of the doctor-patient relationship. Since medical records contain particularly sensitive and intimate information, patients are susceptible to humiliation and discrimination in the event information from their medical records is improperly disclosed. The horror stories are well known, but a few bear repeating:

In Maryland, a banker improperly accessed a medical database to determine which of his borrowers had been diagnosed with cancer. Once such individuals had been identified, the bank improperly attempted to terminate its lending relationship with them.

The chain drug store CVS, and grocery chain Giant Food recently conceded that they had disclosed their customers' prescription records to a direct mail company that then tracked customers and solicited them to consider alternative treatments. After media reports sparked public concern, both companies discontinued this practice.

A study by the University of Illinois found that thirty five percent (35%) of Fortune 500 companies admitted to checking medical records prior to hiring or promoting employees.

A 1997 survey by the American Management Association found that as many as ten percent (10%) of the 6,000 companies surveyed used genetic testing for employment purposes. The Council for Responsible Genetics, a Massachusetts based advocacy group, has documented hundreds of cases in which healthy people have been denied insurance coverage or employment based largely upon genetic "predictions" regarding their future health.

All of these examples involve the use of medical records for a purpose that does not benefit—and indeed may harm—the patient whose records are used. As a general matter in our country, property owned by an individual may not be used by a custodian of the property for any purpose without the owner's consent, and certainly not for a purpose that would harm the owner. But current law does not adequately recognize a patient's "ownership" of his or her medical records.

The ACLU believes that patients own their medical records, and that health care providers or insurance companies who maintain those records should be viewed as custodians of the patients' property. We believe that medical records in the possession of health care professionals or third party payors are like client files in the possession of attorneys. The patient or the client retains ultimate control over the disclosure of information in their records. If follows that (1) patients may reasonably expect that their personally identifiable health information will not be disclosed to anyone unless they have given specific and express written consent, and (2) medical records must be protected from unauthorized access to the fullest extent practicable.

These straightforward objectives are elusive because the United States lacks a coherent and consistent medical privacy policy. A patchwork of state laws affords varying levels of protection to citizens in some jurisdictions. That is insufficient. A nationwide law, such as those under consideration by this Committee, is needed to establish a baseline of medical privacy protections at the dawning of the digital communication age.

Congress itself has recognized the need for federal legislation. As this Committee well knows, the 1996 Health Insurance Portability and Accountability Act includes a provision setting an August 1999 deadline for enactment of a comprehensive medical privacy law. If Congress does not act by that date, the Secretary of Health and Human Services is authorized to enact privacy protections by regulation. With the deadline only four months away, attention is focused on three Senate bills: (1) S. 573, the Medical Information Privacy and Security Act proposed by Senators Leahy, Kennedy, Daschle and Dorgan ("Leahy-Kennedy"); (2) S. 578, the Health Care Personal Information Nondisclosure Act proposed by Senators Jeffords and Dodd ("Jeffords-Dodd"); and (3) a bill soon to be introduced by Senators Bennett and Mack. [1]

The ACLU commends all of the Senators who have introduced or will introduce bills on this subject for seeking to enhance privacy, and we especially applaud Chairman Jeffords for introducing a bill this year that contains significant improvements over the bill he introduced last year, especially in the area of preemption. Nonetheless, the American Civil Liberties Union has formally endorsed S. 573, the Leahy-Kennedy bill, which we believe includes privacy safeguards superior to those contained in the other bills introduced in this and prior Congresses. In the balance of this statement I will explain our decision to support that bill, and propose some additional protections.

II. LAW ENFORCEMENT ACCESS TO MEDICAL RECORDS

I have been asked to focus my attention today on the issue of law enforcement access to medical records, and it is an aspect of the policy debate in which the

[1] We understand that Senators Bennett and Mack may introduce their bill the day before this hearing, too late to be included in this written analysis. The ACLU would be pleased to supplement its submission to include a comparison of the Bennett-Mack bill with the two bills already introduced, if the Committee so requests.

ACLU's preference for the Leahy-Kennedy bill is especially strong. This is true because we believe in the principle, embodied in S. 573, that government agents should be required to obtain judicial approval under a meaningful probable cause standard before they are granted access to medical records containing personally identifiable information.

Both the Jeffords-Dodd and Leahy-Kennedy bills appropriately establish limits on law enforcement access to medical records. Both bills recognize that the computerized medical records of ordinary law abiding Americans are not to be viewed as a centralized law enforcement database like the mugshots or fingerprints of convicted criminals currently maintained by the police. But only Leahy-Kennedy requires law enforcement officers to obtain a court order, or its functional equivalent, before gaining access to medical records, and only Leahy-Kennedy sets a sufficiently high legal standard for such court orders.

Under section 208 of the Leahy-Kennedy bill, a law enforcement agent who wants to view medical records would be required to demonstrate probable cause to believe that (1) the information is relevant and material to an ongoing criminal investigation; (2) the investigative needs of the agent cannot reasonably be satisfied by de-identified health information or by any other information; and (3) the law enforcement need for the information outweighs the privacy interest of the individual to whom the information pertains.

In effect, this legal standard would bring requests for medical records within the protection of the warrant requirement of the Fourth Amendment, notwithstanding the fact that the records are not physically within the possession of the patient. If an individual happens to maintain his or her own x-rays in a desk drawer at home, the Fourth Amendment applies, of course, to an effort by the police to search the desk and seize the x-rays—a search warrant issued by a neutral magistrate based on probable cause would be required. The Leahy-Kennedy bill recognizes that a patient maintains the same ownership interest in x-rays maintained in a doctor's office or in a hospital's computer as in the x-rays kept at home. Applying a Fourth Amendment-like standard to medical records maintained by a third party makes sense, because the Fourth Amendment itself balances the interests of individuals to be secure in their personal papers and effects on the one hand, and the legitimate needs of law enforcement officials on the other.

Moreover, this provision is similar to the protection that Congress has already afforded to individuals with respect to the contents of their electronic communications generally (18 U.S.C. §2703), information pertaining to video rentals (18 U.S.C. §2710), and subscriptions to cable programming (47 U.S.C. §551). Certainly, stored electronic communications, video rental records and cable subscriptions are no less deserving of privacy protection than statements made to a health care provider during the course of medical treatment. Personal medical records should be entitled to no less statutory protection than that currently in federal law for these other everyday transactions.

In addition to establishing a strong legal standard for the issuance of a court order or warrant, the Leahy-Kennedy bill limits the use of protected health information after its disclosure. Specifically, Leahy-Kennedy provides that where protected health information has been disclosed in one investigation, it cannot be used in any other investigation unless the secondary investigation arises out of or is directly related to the investigation for which the protected health information was initially obtained. This balanced approach permits law enforcement officers to conduct legitimate investigations and follow the natural progression of those investigations to conclusion while assuring that protected health information will not be used in an unrelated investigation absent the same type of probable cause proffer that led to the original court order or warrant.

Finally, the Leahy-Kennedy bill contains the important protection of notice to the person whose records are to be searched and an opportunity for that person to contest the appropriateness of the search. It is entirely consistent with notions of due process in our adversarial system of justice that a judge considering whether or not a prosecutor's application for access to medical records meets the legal standard for such access should hear from the other side of the dispute. If there is any risk that notice to the individual would lead to destruction of the records, Leahy-Kennedy permits waiver of the notice requirement. But in an ordinary investigation, notice is appropriate, fair and not unduly burdensome.

As we have noted, the Jeffords-Dodd bill also contains limits on law enforcement access to medical records, but there are four basic reasons why the ACLU prefers the Leahy-Kennedy approach to this subject:

First, while Leahy-Kennedy requires the police to obtain a court order or a grand jury subpoena to access medical records, the Jeffords-Dodd bill permits access to records by means of an administrative subpoena or a summons, neither of which

is reviewed by a court or even issued in the name of a court-supervised body like a grand jury. Administrative subpoenas are typically used by regulatory agencies like the Department of Agriculture or the Occupational Safety and Health Administration to inspect industrial facilities. Summonses are simply demand letters issued on law enforcement stationery. The ACLU believes that personal medical records should not be searched based on summary, self-interested, non-judicial legal instruments such as these. After all, the police are engaged in what Justice Cardozo called the "often competitive enterprise of ferreting out crime," Johnson v. United States, 333 U.S. 10 (1948), and cannot be expected to balance neutrally the competing goals of privacy and law enforcement.

Second, the probable cause standard contained in the Jeffords-Dodd bill is not as comprehensive as its counterpart in Leahy-Kennedy. The standard in each bill requires a showing of relevance, although Leahy-Kennedy calls for a more particularized showing of need. More important, the Leahy-Kennedy standard contains two prongs that Jeffords-Dodd does not—it requires law enforcement to demonstrate that its needs could not be satisfied using de-identified or other information rather than protected health information, and that the need for the information outweighs the individual's privacy interests. These additional prongs in the Leahy-Kennedy standard still fall within a probable cause test, so they do not pose an insurmountable barrier to law enforcement access. But privacy considerations get a fuller airing under the Leahy-Kennedy probable cause standard than under the Jeffords-Dodd probable cause standard.

Third, the law enforcement access section of the Leahy-Kennedy bill, unlike the parallel provisions of Jeffords-Dodd, requires, if practical, prior notice to the individual whose health records are to be searched. The absence of a notice requirement in Jeffords-Dodd is a serious omission in the ACLU's view, because we believe that privacy interests can best be asserted by the person whose privacy is about to be violated. Indeed, we believe that federal law should go a step further than Leahy-Kennedy and require that, where prior notice is not practical, the patient receive after-the-fact notice of the search so that he or she may pursue legal remedies to limit the use of information that has been obtained. But at least Leahy-Kennedy provides for notice and an opportunity to be heard in most circumstances - without notice, a patient's right to privacy in this context will too often remain unarticulated.

Fourth and finally, Leahy-Kennedy more scrupulously guards against derivative use of the private health information obtained by law enforcement. Jeffords-Dodd provides that protected health information obtained by a law enforcement agency may only be used "for purposes of a legitimate law enforcement inquiry." In contrast, Leahy-Kennedy actually prohibits use of the information in any administrative, civil or criminal action against the patient unless the subsequent action arises out of or is directly related to the initial inquiry. In light of the fact that Jeffords-Dodd does not require that the subject of the protected health information be given notice either before or after the disclosure, the absence of any nexus between the initial request and the ultimate use of the records significantly reduces the value of the privacy protection in that bill.

In fairness to the Chairman and Senator Dodd, I hasten to point out that their law enforcement access provision contains at least one important privacy protection that the Leahy-Kennedy bill does not. We welcome section 210(f) of the Jeffords-Dodd bill, which explicitly excludes improperly obtained protected health information from court proceedings. The judiciary would likely find such an exclusionary rule to be implicit in Leahy-Kennedy, but that is not certain, and we therefore urge that this component of the Jeffords-Dodd bill be included in any legislation the Committee ultimately reports to the full Senate. Of course, the value of an exclusionary rule in any privacy bill depends on the extent of the protections that the exclusionary rule enforces, and the Jeffords-Dodd protections fall short, for the reasons already discussed. The ACLU seeks a bill with strong protections and an explicit exclusionary rule to give those protections teeth.

The Chairman's bill also deserves praise because it omits a potential privacy loophole regrettably included in Leahy-Kennedy. I refer to section 208(i) of the Leahy-Kennedy bill, which creates a blanket exception to the bill's protections for information gained while in "hot pursuit" of a suspect. Traditionally, the hot pursuit doctrine has been applied by courts in cases where a suspect might evade arrest or evidence might be destroyed if the police interrupted pursuit to obtain a warrant. That doctrine would seem to have no relevance to an effort to obtain non-mobile evidence such medical records, and in any event is adequately addressed by subsection (d)(2)(B) of the bill, which waives the notice requirement if there is a risk of destruction or non-availability of the evidence. We therefore urge deletion of section 208(i) in S. 573.

Thus far I have listed the ways in which the Leahy-Kennedy bill is generally more protective of privacy vis a vis law enforcement than the Jeffords-Dodd bill, and noted two ways in which Jeffords-Dodd is more protective of privacy vis a vis law enforcement. But that analysis raises a more fundamental query: why should privacy interests ever outweigh the needs of law enforcement? I will answer my own question from three perspectives:

As a former prosecutor, I report to you that law enforcement can function very effectively within a probable cause framework. Respect for the Fourth Amendment and the privacy values it embodies do not unduly hamper police and prosecutors; indeed, in my experience, the exercise of prosecutorial and police power within rules that protect privacy actually increases citizen trust in law enforcement and encourages law abiding behavior. When law enforcement officers are seen as overzealous or overly intrusive, the breakdown in trust and cooperation between government and its citizens has a corrosive and dangerous effect on police and prosecutorial effectiveness.

As a former health policy staffer, I suggest to you that high quality medical treatment relies on candor. Health care providers cannot adequately treat a patient without detailed, intimate information about the patient's medical history and current condition. This is particularly true in such sensitive fields as mental health and substance abuse, where patients may actually avoid treatment altogether if they fear that their treatment records are subject to routine scrutiny. Rules that safeguard the integrity of medical records facilitate the exchange of information between patients and doctors, and that makes for better health care.

Finally, as a civil libertarian, I contend that privacy is itself a value, however intangible, that civilized society must nurture and protect even at the expense of efficient law enforcement. The police would catch a lot more criminals if they could search citizens without cause on the streets and in their homes. But that is not the constitutional system that the Founding Fathers bequeathed to us, and thankfully so.

III. OTHER CIVIL LIBERTIES IMPLICATIONS OF PENDING MEDICAL PRIVACY BILLS

Beyond law enforcement access, the Leahy-Kennedy bill provides more comprehensive privacy protections than other pending medical privacy bills in a number of respects, the most important of which are outlined below:

A. Authorization.

Both Leahy-Kennedy and Jeffords-Dodd require informed consent before patient records are disclosed to third parties, with certain exceptions such as the law enforcement access provisions already discussed. But the Leahy-Kennedy bill approaches the authorization issue in a manner more protective of privacy because the scope of the general release obtained for reimbursement purposes does not extend to "health care operations" or related research carried out within the payor organization. Rather, those activities would properly be subject to regulations regarding health research and concomitant review by an Institutional Review Board.

Leahy-Kennedy also permits patients to exercise a greater degree of control over access to their medical records because the authorization mandated by that bill would inform the patient of the nature of information to be disclosed, the type of person to whom information would be disclosed, and the purposes for which disclosures would be made. In addition, the authorization under Leahy-Kennedy would permit the patient to restrict disclosure of information to certain individuals. Jeffords-Dodd offers no comparable rights.

B. Public Health.

Both Leahy-Kennedy and Jeffords-Dodd appropriately seek to preserve public health functions without unduly infringing on privacy values. Again, however, the ACLU supports the approach set forth in Leahy-Kennedy because it offers individuals greater protection with respect to their medical records. Leahy-Kennedy permits personally identifiable medical records to be disclosed to a public health authority without consent only where the information relates to a specific public health purpose, is reasonably likely to achieve that purpose and cannot be achieved without access to personally identifiable information. Leahy-Kennedy also clearly defines the terms "public health purpose," thereby reducing the risk of improper disclosure.

In contrast, Jeffords-Dodd simply permits the disclosure of personally identifiable health information if it is used for (1) a disease or injury report, (2) public health surveillance, or (3) public health investigation or intervention. Jeffords-Dodd does not require the public health authority to establish any nexus between the personally identifiable information and the purpose of the disclosure. The broad authority

of public health authorities to receive personally identifiable health information under this provision, however well intentioned, is at odds with the expressed purpose of the legislation. The more personal health information in general circulation, the greater the potential for abuse of that information and the less trust between patients and health care providers.

Similarly, while both bills provide for the disclosure of protected health information to health oversight agencies, Leahy-Kennedy takes account of the purpose for which the information will be used, and contemplates safeguards to protect the integrity of health information so disclosed. In contrast, Jeffords-Dodd contains no provision protecting individuals from unwarranted disclosures by an oversight agency. The Leahy-Kennedy bill, therefore, offers superior privacy protection in this regard.

C. Medical research.

High quality biomedical and behavioral research benefits all Americans and is a hallmark of our health care system. Both bills address concerns that new privacy protections might inadvertently impair research activities.

Neither Leahy-Kennedy nor Jeffords-Dodd restricts in any way the use of anonymous or de-identified medical records for research. The bills only regulate research that employs medical records containing personally identifiable information. Moreover, federally funded medical research, clinical investigations using human subjects and certain other research subject to the Federal Policy for the Protection of Human Subjects, are already regulated and, therefore, would not be affected by the pending legislation.

Leahy-Kennedy would apply a uniform standard of accountability and oversight when personally identifiable data is used in either federally funded or non-federally funded medical research. Thus all research using personally identifiable information would be subject to review by Institutional Review Boards ("IRBs"), which currently evaluate whether personally identifiable health information is necessary to a research project that receives federal funding. In contrast, Jeffords-Dodd excludes investigations conducted in connection with "health care operations" from the definition of health research. Thus, under Jeffords-Dodd a managed care provider could use personally identifiable health information for its internal research without review. In addition, under Jeffords-Dodd, use of personally identifiable health information in connection with privately funded research and research supported by commercial entities remains unchecked by Institutional Review Boards.

For privacy purposes, we perceive no basis to differentiate among entities conducting health research using protected health information. Nor should the source of funding control the analysis. Rather, the better rule is to subject all health research to the same minimum standard of review before access to protected health information is granted. The ACLU therefore prefers the research provisions in Leahy-Kennedy.

We wish to propose one additional protection not contained in either bill. The use of even de-identified health information should be limited to the purposes of the Act, including research, and unauthorized use of de-identified information should constitute a violation of the Act. Our concern here is that the de-identification process may not always be absolute; in order to avoid unintended violations of privacy, even de-identified health records should not be recklessly or carelessly disseminated.

D. Civil litigation.

Consistent with the goal of privacy, disclosure of protected health information in civil litigation should occur only after it has been established that the information is material to the adjudication, such as when a litigant has placed his or her medical condition at issue. Both bills provide a mechanism under which protected health information is made available to litigants, but in our view Leahy-Kennedy offers a better balance between the interests of litigants and the rights of non-parties.

Leahy-Kennedy permits a court to order the disclosure of protected health information upon a showing that the information is necessary for the adjudication of a material fact and the need cannot be satisfied using de-identified information. Also, absent exigent circumstances, Leahy-Kennedy requires notice to given to the individual who is the subject of the records before any disclosure occurs.

Under Jeffords-Dodd a court may order disclosure of protected health information after a litigant has established that presentation of its claims or defenses would be impaired without the information. The ACLU believes that this lower standard is insufficient to outweigh the important privacy rights of the patient whose records are sought. However, Jeffords-Dodd directs the court to impose specific obligations on the parties to the litigation in order to protect the privacy of the medical records, an important refinement not present in Leahy-Kennedy.

E. Preemption.

The ACLU strongly supports the non-preemption policy embodied in the Leahy-Kennedy bill. While the Jeffords-Dodd bill preempts far fewer state laws than the bill introduced by the Chairman last Congress, it would unacceptably preempt efforts by states to enact more stringent privacy laws in the future.

It has been argued by others that preemption of state medical records privacy laws is necessary to avoid confusion over which state law applies in an era of nationwide health care plans and insurance companies. But the Leahy-Kennedy bill solves that problem by establishing the principle that patients own their own medical records. Therefore, the domicile of each patient serves as a concrete reference for the determination of whether additional privacy protections enacted by a particular State would apply. Under Leahy-Kennedy, a State would remain free to address privacy needs—some local in nature—that may arise in the future.

As a rule, federal privacy laws outside the health care arena—such as those described earlier in this testimony—have not preempted state laws. The examples of coexisting Federal and State regulations are legion, and there is simply no justification for usurping the longstanding rights of States to legislate privacy protections for their citizens. Any federal law should set the foundation upon which privacy protections rest without inhibiting states from acting to enhance those protections.

IV. CONCLUSION

For the reasons described above, the American Civil Liberties Union has endorsed S. 573, the Leahy-Kennedy medical records privacy bill. But we again wish to praise Chairman Jeffords and all the other members of the Senate who have taken steps to address this important subject, and we look forward to working with the Committee to make sure that a strong medical records privacy bill is signed into law prior to the August deadline.

Response to Questions of Senator DeWine From Ronald Weich

Question 1. In most States there are "mandatory reporting" laws that require health care providers, among others, to report medical conditions that are possibly indicative of criminal activity. In Ohio, for example, we require that suspicious wounds caused by gunshots or stabbing be reported. In both instances, good faith reporting immunizes the reporting individual from liability. How do we balance protecting children from abuse (under State mandatory child abuse and neglect laws) with medical records privacy concerns? How should we recognize the State mandatory reporting laws?

Answer 1. The ACLU has no objection to current laws requiring health care providers to alert state or local authorities when they treat gunshot wounds, child abuse, or other injuries that suggest violent criminal activity. Each of the bills pending before the Committee contains an express exception for "Public Health" which would permit the collection of such information without the prior written consent of the patient. Specifically section 207 of the Jeffords-Dodd bill (S. 578) provides that a health care provider "may disclose protected health information to a public health authority or other person authorized by law for use in a legally authorized (1) disease or injury report." The Bennett-Mack bill (S. 881) contains a substantially identical provision.

We believe, however, that the Leahy-Kennedy bill (S. 573) strikes the most appropriate balance between law enforcement and privacy concerns in this context. Section 205(b) of the Leahy-Kennedy bill is similar to the Public Health exceptions in Jeffords-Dodd and Bennett-Mack, but it defines "Public Health Purpose" with greater specificity than the other bills, and it requires that any disclosure to a public health agency (1) relate to a specified public health purpose, (2) be reasonably likely to achieve such purpose, and (3) cannot be satisfied with de-identified information. These requirements do not present an insurmountable barrier to the reporting of personal health information when needed to protect public health, but they require common sense scrutiny of public health activities similar to those applied to health researchers elsewhere in the bill to ensure that health care privacy is violated to the minimum extent necessary.

It is appropriate for protected health information to be revealed to government officials pursuant to mandatory reporting laws if they meet the straightforward test in Leahy-Kennedy. We are confident that current laws pertaining to gunshot wounds and child abuse meet that test, and they would continue to be enforced after enactment of that bill or the other pending bills.

Question 2. A rapist flees from the scene of an attack and severely cuts his arm on a broken glass door. Now police notify all medical treatment facilities in the locality to be on the lookout for an individual looking for treatment for a gash on the

arm. Because of the general description of the suspect and wound and the number of medical facilities alerted, there is a lack of specificity to obtain a warrant. How should this be dealt with under privacy standards? Should medical personnel be allowed to respond to the police request for help?

Answer 2. Adoption of a medical records privacy bill would not hamper law enforcement in its effort to catch criminals. Each of the bills before the Committee contains sensible exceptions to grant the police access to medical records when needed to serve the legitimate needs of law enforcement, but the bills generally require that when such records include personally identifiable information, access must occur pursuant to legal process and review by a neutral magistrate.

In Senator DeWine's hypothetical, the police may want to find out whether or not a hospital has treated individuals for a particular wound. This question is permissible without legal process, because the information sought is not "protected health information"—it does not seek the identity of individuals. Thus law enforcement officers would be free to contact various medical emergency rooms and health care facilities and ask whether anyone presented for treatment at those facilities with the particular injuries. Once officers determined which, if any, health care providers treated the specified injuries, they could seek a search warrant directing the health care provider to release the identities of the individuals treated. And once they have probable cause to believe that the records of any individual contain evidence of a crime, they may obtain a warrant for those records.

The Justice Department testified at the hearing that federal prosecutors believe good practice requires them to seek a warrant in order to obtain the actual medical records. The pending legislation merely requires them to do what they already acknowledge to be good practice. This practice comports with the Fourth Amendment, and Congress should clarify that the privacy protections of the Fourth Amendment extend to an individual's personally identifiable health information.

Additionally, section 208(i) of Leahy-Kennedy expressly exempts information released to law enforcement officials while they are in "hot pursuit" or if other exigent circumstances exist. Although the ACLU believes that this exception is overly broad in its current form, language could be crafted to conform with the traditional "hot pursuit doctrine" which applies in cases where a suspect might evade arrest or evidence might be destroyed if the police interrupted pursuit to obtain a warrant. The ACLU believes that subsection 208(d)(2)(B) of the Leahy-Kennedy bill, which waives the notice requirement if there is a risk of destruction or non-availability of the evidence, sufficiently embodies the hot pursuit doctrine. Accordingly, section 208(i) is superfluous.

This analysis of the pending legislation is consistent with the treatment of analogous situations by courts. For example, in Mississippi v. Baptist Memorial Hospital-Golden Triangle, 726 So. 2d 554 (Miss. 1998), it appeared that the perpetrator of a homicide had been injured at the scene of the crime. Accordingly, law enforcement officers secured a grand jury subpoena directing Baptist Memorial Hospital-Golden Triangle (BMH-GT) to turn over to law enforcement officers the names and addresses of all individuals presenting for treatment of all cuts and lacerations. BMH-GT refused to comply with the subpoena, citing patient confidentiality.

Law enforcement officers then obtained a search warrant seeking the same information. BMH-GT again refused to comply and filed a petition to quash the subpoena and the warrant. Although the trial court granted BMH-GT's motion to quash, on appeal the Mississippi Supreme Court reversed and ruled that the patient-physician privilege could not be used as a cloak for a crime, particularly where the hospital was required under separate statutes to report the information to public health authorities. In reversing, the Mississippi Supreme Court made clear that law enforcement officers would not be free to "go on a fishing expedition" in the patient records. Therefore, de-identified information was to be provided in response to the warrant. Then, after law enforcement officers identified one or more probable suspects, they could obtain a warrant for the identifying information.

As discussed more fully in my hearing testimony, respect for the Fourth Amendment and the privacy values it embodies does not unduly restrict police and prosecutors. Rather, the exercise of prosecutorial and police power within rules that protect privacy actually increases citizen trust in law enforcement and encourages law abiding behavior. Overzealous law enforcement activities erode trust and cooperation between government and citizens and hampers police and prosecutorial effectiveness.

Response to Question of Senator Wellstone From Ronald Weich

Question. I am asking this question of you because you are a former Federal prosecutor and have been involved in numerous judicial reviews in your capacity as a prosecutor.

Our understanding is that in practice, law enforcement officials now obtain a court order to access medical records. Do you think we should break precedent with all other privacy laws and allow law enforcement to gain access to probably the most sensitive personal information without some legal process? Can you give us instances in your experience as a Federal prosecutor in which law enforcement sought a court order for medical records and was denied, and the denial thwarted the success of their investigation?

Answer. At the outset, I must clarify that I was not a federal prosecutor. From 1983 to 1987, I served as an Assistant District Attorney in New York City; I prosecuted criminals in state court, not federal court.

Law enforcement efforts are not hampered by the requirement that they obtain a warrant before gaining access to medical records. The warrant requirement in the Fourth Amendment applies to searches of other personal papers and effects, and it has served the country well for over 200 years. The only reason the Fourth Amendment does not apply to medical records is that these records are typically not held by the patient, but by doctors, hospitals and insurers.

The privacy protections in the Leahy-Kennedy and Jeffords-Dodd bills are not radical. They largely codify current state law practice. A cursory review of the case law indicates that unless law enforcement officers to obtain a warrant or an investigative subpoena for medical records they are not admissible as evidence in a criminal proceeding and information derived from the records in suppressed. See e.g., State of Montana v. Nelson, 283 Mont. 231 (1997) (refusing to quash investigative subpoena issued with probable cause); Commonwealth v. Shaffer, 714 A.2d 1035 (1998) (suppressing evidence obtained as the result of a warrantless search of defendant's medical records); Illinois v. Wilber, 279 Ill. App. 3d. 462 (1996) (permitting introduction of evidence obtained from defendant's medical records where law enforcement had complied with statutory provisions for the release of the information); Mississippi v. Baptist Memorial Hospital-Golden Triangle, 726 So. 2d 554 (1998) (finding defendant had no greater expectation of privacy in his medical records than in his residence which could be searched pursuant to a valid warrant). Thus, it would actually break with precedent to permit law enforcement officers to have unfettered access to medical records.

Based on my experience as a prosecutor, I can report that it is not unduly burdensome to obtain a search warrant in a timely manner. Such warrants are commonplace. I am personally aware of no instance in which a proper law enforcement application for access to medical records was refused in the course of a criminal investigation. We have also reviewed relevant case law, and although defendants sometimes moved to quash the warrants or subpoenas pursuant to which law enforcement officers obtained their records, we identified only one instance in which the defendant's motion was successful. Montana v. Dolan, 283 Mont. 245 (1997). However, in that case, the investigating officers had no personal knowledge which would be sufficient to support the issuance of a warrant. In addition, the officers did not know the identity the witnesses, and therefore were unable to offer any evidence regarding the reliability of their statement. The Montana Supreme Court concluded there was insufficient basis for the issuance of the warrant pursuant to which the medical records had been obtained and ordered evidence obtained pursuant to the warrant suppressed.

The ACLU believes that the Leahy-Kennedy bill properly balances the interests of individuals in the privacy of their medical records and the legitimate need of law enforcement officers to access those records in connection with criminal investigations. The Justice Department approach of allowing unchecked access to medical records by law enforcement officials would significantly reduce the privacy afforded to medical records in many states. In contrast, legislation that safeguards the integrity of medical records will facilitate the open exchange of information between patients and doctors, and thereby improve the quality of health care.

The CHAIRMAN. Professor Shapiro.

Ms. SHAPIRO. Mr. Chairman and distinguished committee members, thank you for this opportunity to present the views of the American Bar Association regarding legislation to protect the privacy of health care information, particularly as it affects law enforcement interests and needs.

I serve on the governing board of the ABA's Section of Individual Rights and Responsibilities, and I previously chaired that section's Health Rights Committee, which originated ABA policy in this area. As you mentioned, in addition, I am a professor of bioethics

at the Medical College of Wisconsin where I direct the Bioethics Center, and I practice health law in a large Milwaukee firm, and I have had experience with some of the law enforcement activities that have been mentioned here today. Much of my practice and my academic work actually focuses on health information privacy concerns.

In my mind, and as was alluded to by Senator Frist today, these concerns are and must be at the center of the larger debate on health care that has engaged this country for the past several years, because health information privacy does and must anchor the doctor-patient relationship and the public's trust in our health care delivery system. And I am going to go back and reiterate some of this, although I believe there is consensus in the room.

We have to again acknowledge that health information is uniquely personal and sensitive and that records contain not only detailed information about the conditions and the treatment and the medication that patients get, but information about patients' families, information about mental illness, information about dietary habits, employment status and the health care providers' subjective impression of the patient's character, personality and mental State.

With advances in genetic capabilities, many patients' medical records now also contain genetic test and treatment information, which often discloses probablistic information not only about them but about their parents, about their children and about their siblings.

Patients do fear disclosure of this sort of information to their employers and insurers and school officials and mortgage lenders and other entities that could use this information against them.

Unfortunately, these fears are not unwarranted. Recently, a pregnant woman who underwent cystic fibrosis testing which was positive was informed by her insurance company that they would not pay for her child's health care costs if she chose to continue the pregnancy.

In another case, a woman whose mother had breast cancer was told that her own health care coverage would exclude treatment of that condition.

In another case, a man who underwent screening for colon cancer as part of a research protocol ended up losing his health insurance.

In response to these fears and these real dangers, many patients are insisting that their physicians treat them anonymously on a self-pay basis, with no documentation at all. Some, as has been mentioned today, are avoiding tests or withholding critical information about their habits and their conditions.

Sometimes, patients decide not to seek treatment at all or not to enroll in clinical trials, and physicians for their part, fearing that their medical records may be accessed and used to create a database for purposes other than good patient care, feel pressured to fudge what they put in a record or not to put critical information in at all.

And all of this increases the risks of misdiagnosis, inadequate care and stymied medical research. We are all then deprived of the benefits of both public health information and enhanced medical knowledge.

This past February, in response to advances in genetics, advances in computerized health information capabilities and the growing significance of the disparities among State information privacy laws, the ABA supplemented its existing health information privacy policy. The salient provisions of our policy affirm our strong support for legislation at the Federal level which would ensure that confidential, personally identifiable health information is not disclosed without informed, voluntary, written authorization except for specific and limited purposes, including certain properly circumscribed disclosures to law enforcement; that those who have this sort of health information have a continuing obligation to refrain from misusing it; and that effective tracking and enforcement mechanisms are in place.

We recognize that the privacy of health information is not absolute and that law enforcement agencies do need access to this information, as was said earlier, primarily for two purposes—investigating potential cases of fraud and to investigate specific individuals in matters unrelated to fraudulent activity.

I think we have to look at the disparity in State laws that currently govern that access. In some States, law enforcement officials are free to search through patients' medical records without any legal process at all. In other States, law enforcement officials use compulsory process in the form of a warrant or subpoena to get medical records. In the first instance, clearly, there is no protection, and in the latter, the thresholds for obtaining the information vary considerably. Some States require prior judicial approval for certain subpoenas; some do not.

At the Federal level, an agent who seeks to obtain a grand jury subpoena for access to medical records simply has to convince the prosecutor that the information sought is relevant to the scope of a pending grand jury investigation, which is a bar so low that it really offers almost no protection at all. There is no judicial oversight in these circumstances unless the recipient of the subpoena refuses to comply, in which case there is a motion for a court order to compel, and even then, protection is very limited.

I see the red light is on.

The CHAIRMAN. Take another minute or two.

Ms. SHAPIRO. Thank you.

Where health information is obtained pursuant to a subpoena, I think we also have to acknowledge that there is no guarantee that this information is going to be used for the purpose for which it was obtained. Evidence that is shown to a grand jury is sealed for secrecy, but information that is obtained but not shown to the grand jury is not sealed and can then be used for other purposes.

As early as 1977, the Privacy Protection Study Commission recognized this fundamental gap in privacy protection, concluding that a grand jury subpoena had become little more than an administrative tool.

There is no comprehensive law today that guards against these kids of threats to privacy. We need one. Of the three major health information proposals currently before you, we believe that S. 573 is the most consistent with our ABA health information privacy policy provisions, although, Mr. Chairman, yours comes very close as a runner-up.

The CHAIRMAN. It may just win, too.

Ms. SHAPIRO. We are particularly concerned about two aspects of the Leahy proposal that have not been focused on today, having to do with destruction or return of material once it is obtained, and with limited use of this material for unrelated purposes. We need uniform minimum national standards for privacy and confidentiality, and I encourage and applaud you for your work.

Thank you, Mr. Chairman.

[The prepared statement of Ms. Shapiro follows:]

PREPARED STATEMENT OF ROBYN S. SHAPIRO

Mr. Chairman and distinguished Committee members, thank you for this opportunity to present the views of the American Bar Association (ABA)[1] regarding legislation to protect the privacy of health care information, particularly as it affects law enforcement interests and needs.

ABA President Philip S. Anderson asked me to testify on his behalf today because of my longstanding involvement with health records privacy issues. I serve on the governing board of the ABA Section of Individual Rights and Responsibilities and previously was chair of the Section's Health Rights Committee, which originated the ABA's policies in this area. In addition, I am a professor of Bioethics at the Medical College of Wisconsin, Director of the College's Center for the Study of Bioethics, and a partner in the Health Law Practice Group of Michael Best & Friedrich LLP, a large law firm in Milwaukee. Much of my practice and academic work focuses on health records privacy concerns.

ABA Policy Regarding the Confidentiality of Health Care Information

The ABA has had policy addressing certain aspects of the privacy of health care information for several years. This past February, the ABA supplemented existing policy with an additional statement developed to address recent advances in genetic capabilities, the increasing prevalence of computerized health information, and the growing significance of disparities among state health information privacy laws. The ABA's most current health records policy was drafted only after thorough research of the issues and careful consideration of the opinions of experts in relevant fields. It was adopted by the House of Delegates, the ABA's policymaking body, after open debate on the issue.

The salient provisions of the ABA's policy (see attachment) affirm our strong support for federal legislation that would ensure that:

(1) Confidential, personally identifiable health information is not disclosed without informed, voluntary, written authorization except for specific and limited purposes—including when disclosure is necessary to comply with:

(a) a court order;

(b) a proper discovery request or subpoena; or

(c) other constitutional request by a law enforcement or regulatory agency;

(2) Those who possess personally identifiable health information have a continuing obligation to refrain from misusing it; and

(3) Disclosures of personally identifiable health information are tracked; and

(4) Parties who violate the law knowingly or, in the case of corporate entities, with reckless disregard, are subject to meaningful penalties.

Of the three major health information privacy proposals currently under consideration by the Senate, S. 573, the "Medical Information Privacy and Security Act," is most consistent with these policy provisions. Specifically, in accordance with ABA policy, S. 573 would limit disclosure of health information to investigative or law enforcement officials to circumstances where disclosure is necessary to comply with:

(a) a warrant;

(b) a grand jury subpoena; or

(c) a court order, following proper notice, based on showing probable cause to believe that:

(i) the health information sought is relevant and material to an ongoing criminal investigation;

(ii) the needs of the officer cannot be satisfied by de-identified health information or any other information; and

---

[1] The ABA, the world's largest professional organization, with more than 400,000 members, is the national representative of the legal profession, serving the public and the profession by promoting justice, professional excellence, and respect for the law. The Section of Individual Rights and Responsibilities focuses on civil rights, civil liberties, and human rights concerns.

(iii) the law enforcement need for the information outweighs the privacy interest of the individual to whom the information pertains.

In addition, by prohibiting use of disclosed protected health information in subsequent, unrelated legal actions or investigations and by requiring the destruction or return of disclosed health information at the conclusion of the matter for which it was disclosed, S. 573 accords with ABA policy provisions imposing upon those who possess health care information a continuing obligation to refrain from misusing it. Finally, the bill's provisions concerning the availability of criminal and civil penalties in individual causes of action satisfy ABA policy requirements for meaningful redress for violations of the law. We believe that by requiring that disclosure of health information occur only in appropriate and carefully controlled circumstances, these provisions strike an appropriate balance between the need to safeguard the privacy of health information and the need to facilitate legitimate law enforcement investigations.

The Need for Health Care Information Privacy

Health care information is uniquely sensitive and personal. Typically, patient records contain detailed information about the patient's history of diseases, tests, treatments and medications; the patient's family members medical history; any history of substance abuse or mental illness; the patient's dietary habits; the patient's employment status and income; and the health care provider's subjective impressions of the patient's character, personality and mental state.[2] With rapid advances in genetic capabilities, many patients' medical records now also contain genetic test and treatment information that often discloses not only probabilistic information about the patient's future, but also personal data about the patient's siblings, parents, and children. Unwarranted disclosure of health-related information can be devastating both to the patient and to others associated with that person. For example, genetic information about an individual is particularly susceptible to misuse because it can reveal medical facts about future health risks of the individual and the individual's relatives. Unauthorized disclosure of such information already has led to documented cases of discriminatory treatment by potential employers and insurers.

Equally important, however, disclosure can have significant public health consequences; individuals who fear that their privacy will not be respected[3] are less likely to discuss their conditions or risky behaviors candidly with their health care providers. In some instances, they may decide not to seek treatment at all and not to participate in clinical trials. They thereby increase the risks of misdiagnosis, inadequate care, and stymied medical research and deprive themselves-and all of us-of the benefits of both public health information and enhanced medical knowledge.

Disclosure of Health Care Information to Law Enforcement

Law enforcement agencies seek access to personally identifiable health information primarily for two purposes. First, prosecutors and agencies rely on individual patient records when investigating potential cases of fraud in the health care industry. Although the targets of fraud investigations usually are the health care providers and payors, investigators often review patient records to confirm the fraudulent activity. Second, law enforcement officials use health information to investigate specific individuals in matters unrelated to fraudulent activity.[4]

In some states, law enforcement officials are free to search through patients' medical records without any legal process at all. In other states, law enforcement officials use compulsory process, in the form of a warrant or subpoena, to obtain patients' medical records.[5] In the first instance, there clearly are no privacy protections for individuals' records; in states requiring warrants or subpoenas, the thresholds for obtaining the information vary considerably. For example, while some states require prior judicial approval for the issuance of certain subpoenas, others impose no such requirement. And at the federal level, an agent who seeks to obtain a grand

---

[2] See Office of Technology Assessment, "Protecting Privacy in Computerized Medical Information" (1993).

[3] Surveys consistently indicate that Americans are worried about access to and use of personal information by others, and that the privacy of health-related information is of particular concern. See Equifax/Harris Consumer Privacy Study (1995), in which 80% of respondents said that "consumers have lost all control over how personal information about them is circulated and used by companies" and Equifax/Harris Health Care Information Privacy Survey (1993), in which 85% of the respondents said that the confidentiality of health data is "absolutely essential" or "very important."

[4] See Barefoot, B., "Enacting a Health Information Confidentiality Law: Can Congress Beat the Deadline?" 77 N.C. L. K-e-v. 283, 341 (1998), Ejljag Robert S. Litt, Deputy Assistant Attorney General, Testimony on Behalf of the U.S. Dept. of Justice Before the Subcommittee on Privacy and Confidentiality of the Naf I Comm. on Vital and Health Statistics 10 (Feb. 18, 1997).

[5] Id.

jury subpoena to access medical records need only convince a prosecutor that the information sought is relevant to the scope of a pending grand jury investigation,[6] a bar so low that it is not really a safeguard at all against inappropriate or unnecessary disclosure. In these circumstances, there is no judicial oversight unless the recipient of the subpoena refuses to disclose the information, in which case officials must seek a court order to compel disclosure. Even when such an order is required, however, protection is limited; if the subpoena has been served on a physician being investigated for fraud, for example, the physician's patients may not have the necessary standing to challenge the subpoena.[7] And because grand jury subpoenas entail no notice requirements, the patient may never even become aware that law enforcement officials have obtained personal information from the physician.[8]8

In cases where health care information is obtained pursuant to a subpoena, there is no guarantee that the information will be used only for the purpose for which it was obtained. Although evidence that is shown to a grand jury is sealed for secrecy, information obtained but not shared with the grand jury is not sealed and could be used for other purposes.[9] As early as 1977, the Privacy Protection Study Commission, recognizing this fundamental gap in privacy protection, concluded that the grand jury subpoena had become "little more than an administrative tool" by which law enforcement could access records without having to satisfy the search warrant probable cause standard.[10] This criticism since has been echoed in, e.g., Thurman v. Texas, 861 S.W. 2d 96, 101 (Tex App 1993), where the court stated, "The unrestricted use of grand jury subpoenas to obtain medical records is a serious threat to privacy. There is almost no limit on what can be obtained without the knowledge or approval of any court, any grand jury, . . . or the person affected."

As you know, there is no comprehensive law that guards against these kinds of threats to individuals' privacy by providing significant protections for health-related information. Yet the need for such protections is evident to the medical community, the legal profession, and even the general public. Inappropriate and damaging access to information is being documented by the media. For example, in August 1998, The Washington Post reported that in Fairfax, Virginia, just outside our capital city, police investigating a car theft secured a warrant from a county magistrate to seize the medical records of 79 drug-treatment patients because they attended a clinic 200 yards from the location where the vehicle disappeared. The police gave no reason to suspect anyone connected with the clinic. In his affidavit requesting the warrant, the detective stated that obtaining the records was necessary because "[i]t is common for people who have addiction of various narcotics . . . to engage in these kinds of criminal activities to support [their] drug addictions."[11] Following the clinic's petition to the court for return of the records (but prior to court action on the matter), the police conceded that their search warrant was not appropriate.[12]

The ABA of course recognizes that law enforcement agencies do need access to health record information in some circumstances and that obtaining such access should not be so burdensome that it thwarts legitimate investigations. However, we do not believe that the safeguards proposed in S. 573 or similar legislation would pose any such burden; on the contrary, they are necessary to ensure minimum privacy protections for all.

Both the ABA policy and provisions of the "Medical Information Privacy and Security Act" outline ways in which any tension between the individual's right to privacy and society's interest in effective law enforcement can be resolved through clear legislative delineation of 1) the specific circumstances in which law enforcement officials may access protected health information; 2) the probable cause criteria and notice requirements for the issuance of court orders for disclosure of such information to law enforcement; 3) restrictions on use of such information for other law enforcement inquiries; 4) requirements for destruction or return of the information at the conclusion of the matter for which the information was disclosed; and 5) meaningful penalties for violations of the law.

---

[6] Id.

[7] United States v. Miller, 425 U.S. 435 (1976) suggests that courts may be reluctant to recognize individuals' protected interest in information about them held by a third parry.

[8] See Privacy Protection Study Commission, "Personal Privacy in an Information Society" 282, 366 (1977).

[9] See Barefoot, supra n. 4 at 34 1, citing Privacy Commission, id., and Litt Testimony, supra n. 4.

[10] See Privacy Commission, supra n. 8 at 377.

[11] Masters, B., "Fairfax Police Criticized for Seizing Clinic Files," The Washington Post, Aug. 28, 1998.

[12] Masters, B., "Fairfax Police Concede Seizure Was Wrong", The Washington Post, Sept. 1, 1998.

In fact, precedent for these sorts of restrictions already exist in other contexts. For example, current federal law requires a law enforcement agency to obtain a court order before accessing personally identifiable information concerning a cable television subscription, and such a court order may not issue unless officials establish by "clear and convincing" evidence that the information sought is material to the investigation for which the information is being sought.[13] Surely, no one can disagree that the confidentiality of health-related information deserves at least as much protection as our choices in television viewing.

Indeed, the intimate nature of health records information and the potential ramifications of its misuse require a special response in the law. In this area, it is simply not enough to impose penalties for misuse of health information by law enforcement. First, it is unlikely that punishment—always administered after the fact—will reassure the public that unlawful access to or use of information won't occur again. As noted by Dr. Marcia Goin, Clinical Professor of Psychiatry at the University of Southern California School of Medicine, "People don't feel safe in their homes Dust] because their state has enacted the death penalty. Similarly, public trust in protection of medical information privacy will not be supported by the enactment of harsh punishments for the misuse of patient information."[14] More important, however, protection of such information should be affirmative, proactive, and as comprehensive as possible to ensure that inappropriate access or use is unlikely in the first instance.

Conclusion

Protecting the confidentiality of personally identifiable health information is critical to safeguarding the trust in the patient-physician relationship and promoting the public's trust in our country's health care delivery system. Federal legislation that establishes a uniform, minimum national standard for privacy and confidentiality of health information is essential to accomplish that objective. This standard must guard appropriately against law enforcement agencies' overbroad access to health information while taking into account their need for access in accordance with established processes and constitutional guarantees. In the end, any system that fails to assure such protection will undermine the public's trust and thereby fail to maintain public's support. Such failure will create the unacceptable risk that we, as individuals, will withdraw from full and honest participation in our own health care decisionmaking.

AS APPROVED BY THE ABA HOUSE OF DELEGATES FEBRUARY 8, 1999

AMERICAN BAR ASSOCIATION

SECTION OF INDIVIDUAL RIGHTS AND RESPONSIBILITIES

COMMISSION ON LEGAL PROBLEMS OF THE ELDERLY

RESOLUTION

Resolved, that the American Bar Association supports federal legislation that explicitly acknowledges individuals' rights to privacy of their health care information and that protects the confidentiality of personally identifiable health information from any source, including medical records, electronic data, and genetic material, and ensures that:

1. individuals have the right to prevent others from generating personally identifiable health information about them without their consent;

2. individuals have the right to see, copy, and correct their personally identifiable health information and to delegate this right to others;

3. disclosure of personally identifiable health information is not permitted without informed, voluntary, written authorization by the individual who is the subject of the information, except for limited, specific purposes where it is reasonably determined that disclosure is necessary (a) to prevent serious jeopardy to the life or health of the individual; (b) to allow for the sharing of information among the individual's caregivers; (c) to process a claim for payment for health care services or insurance benefits received by the individual; (d) to comply with a court order, proper discovery request or subpoena, or other constitutional request by a law enforcement or regulatory agency; (e) to enable a health care provider to obtain advice of counsel directly related to health care services provided to the individual (subject to coun-

---

[13] "See 47 U.S.C. Sec. 551 (h) (1994).

[14] Skolnick AA, "Opposition to law officers having unfettered access to medical records," JAMA, 279 (4): 257-9, Jan. 28, 1998.

sel's continuing duty to refrain from further disclosure); or (f) to comply with applicable law;

4. disclosures of personally identifiable health information are tracked;

5. those who possess personally identifiable health information have a continuing obligation to refrain from misusing it; and

6. parties who violate the law knowingly or, in the case of corporate entities, with reckless disregard, are subject to meaningful penalties, and a person aggrieved by a violation of the law has a private right of action.

Further Resolved, That the American Bar Association encourages, in the absence of a federal legislative mandate, the development of strong institutional and organizational policies that adhere to the above principles to protect the privacy and confidentiality of doctor/patient communication and protect against misuse of personally identifiable health information.

The CHAIRMAN. Thank you. All of the Senators that you have seen this morning are going to be working together to come up with the solution, and we deeply appreciate your comments.

We heard testimony earlier that the Department of Justice supports the recommendations made by the Secretary of Health and Human Services in 1997 with regard to law enforcement. What is your position on the Secretary's recommendations, Mr. Weich?

Mr. WEICH. Mr. Chairman, we are very concerned by those recommendations. We do not think they afford adequate protection to the American people in this important area. The Justice Department testimony this morning was striking in several respects. First of all, I can say that each of the examples that they posed where they would like to obtain access to information, I believe they could obtain under the bills that are before the committee.

For example, the example of the rapist who injured his hand and was going to be treated at a local hospital—the nonidentifiable request by law enforcement agents of local hospitals, did you treat somebody for a hand injury, is not one that I believe is considered protected health information under your bill, Mr. Chairman. So that simple inquiry, which does not ask for any names, could clearly be provided by the hospital.

In any event, as Mr. Bentivoglio conceded, the law enforcement agent would need to get a warrant after that. If they are finding out in Washington area hospitals on a particular night that some people were treated for hand injuries, they are going to have to go before a court, and a judge should have to weigh whether the specificity of the information that is sought and the seriousness of the crime outweigh the invasion of privacy that innocent bystanders will suffer. I think that on the facts that were presented, given the relative specific nature of this injury, the nonintimate nature of the health care that was sought by various people with hand injuries, and the serious nature of the crime—namely, rape—a judge might well issue a warrant.

And it is not that difficult to obtain a warrant. I myself, when I was an assistant district attorney, obtained search warrants in less than an hour. It is really that simple. Much of the work is already prepared because these cases are fairly routine, and the fact patterns tend to recur.

In a more complicated case where there is a close question, it might be that you need to put in more work. If time is of the essence in getting the information, as Senator Reed pointed out, there are provisions in the bill that provided for immediate access to law enforcement. In both bills, there is a provisions that says if

someone is in imminent danger of serious injury, of course, we are going to permit access to records to prevent that injury. But if it is something that can wait a couple of hours so that a neutral magistrate can consider the facts and weigh, on the one hand, law enforcement's needs against the interests of privacy, that is what should happen under our constitutional system of government.

The CHAIRMAN. Dr. Shapiro.

Ms. SHAPIRO. I agree with much of what was said and have two additional comments. We need uniformity, and we need laws if only for that. Second, there are abuses. Some anecdotes are included in my written testimony. We have heard some from Senator Frist this morning. But maybe most importantly, and this is based on my own experience in my health law practices, theoretically—and I am making no allegations here—but theoretically, the danger of abuse and invasion of privacy when the request is from law enforcement is all the more heightened on account of the often intimidating nature of the request.

People with whom I deal as clients for the most part are law-abiding citizens who are scared to death when the people with the windbreakers come in and say, "Let me see your medical records."

So we need to be sure that people know the ground rules, that they know how they can best protect their patients' privacies while facilitating appropriate law enforcement requests.

The CHAIRMAN. Mr. Weich, you advocate a requirement that law enforcement must give prior notice to the individual whose health records will be investigated. Law enforcement officials who investigate Medicare billing fraud believe such a requirement would be extremely burdensome and would indicate suspicion of a provider before any charges have been brought.

How do you respond to that?

Mr. WEICH. First of all, Mr. Chairman, it is important to distinguish between the law enforcement access provisions in both bills, all bills, and the health oversight provision. The kinds of routine audits of health care billing records that are going to occur will I think occur under the health oversight provisions, and there, there is no need for prior notice; that is just going to go on in a routine way. Much of that, incidentally, can occur using de-identified information. So again, there is no privacy interest implicated and no need to provide notice to anybody else.

If you are talking about a specific law enforcement investigation of a particular person, and if the exceptions in the Leahy-Kennedy bill are not present, yes, we believe that notice is important. In our adversarial system of justice, we believe that the person whose interests are directly implicated—the owner of the medical records—should have an opportunity to contest the probable cause that is asserted by law enforcement, and in particular cases, that will be heard by a judge, and the judge will make a determination. It happens every day in courts throughout the country.

The CHAIRMAN. Thank you.

Senator Reed.

Senator REED. Thank you, Mr. Chairman.

I want to thank the witnesses for their testimony. First, I think something we can agree upon, and Professor Shapiro, you seem to say it very explicitly, is that there is a need for a Federal standard

that would essentially clarify for every State privacy responsibilities with respect to medical records. I would assume you would agree with that.

Mr. WEICH. Yes, although— I want to emphasize that the ACLU opposes preemption of State laws—we think there should be a Federal floor.

Senator REED. Let me get back to the law enforcement issues which I was talking about with the officials from the Department of Justice. I think we all recognize that there are fundamental privacy rights, but we also recognize that there are fundamental law enforcement concerns. And getting back to the example which was presented about searching the emergency rooms, from your previous comment to the chairman's question, Mr. Weich, you seem to imply that they could ask for information without any personal connection. They could ask, "Did you treat somebody?"

Mr. WEICH. First of all, Senator, it strikes me as an unnecessary step. Taking the example as it is specifically presented, in the Washington area, there were people treated for hand injuries at every hospital every night, and so I would not think that law enforcement needs to go around asking that general question. What they want to do is find out if a person matching a particular description was treated for this kind of hand injury, and if so, who was that person, and that that is asking for personally identifiable information, and we think that law enforcement should have to seek a warrant for that information.

Senator REED. Well, it seems to me, again, that this is an area where both absolute positions are going to yield openly to some type of practical arrangement. That is what we do. That is our job.

It seems to me that if there is a crime committed, and you know the perpetrator has been injured, probably seriously enough to get medical care, you have a rough description of the person, that logically, a police official would go into treatment centers and ask, "have you seen this person?" Are you telling me that your view would be that the hospital, even if they know that, would say they could not provide that information, forcing the police to go back and get—what would they have to get?

Mr. WEICH. I think they would obtain a search warrant.

Senator REED. So they would have to go and get a search warrant to come back an establish that——

The CHAIRMAN. Just to identify that a person had been there?

Mr. WEICH. No, no. As I said, the initial inquiry, which does not call for personally identifiable information—was somebody treated; did you treat people——

Senator REED. But again—excuse me—I guess the question here, really, and I think it is the chairman's question, too, is they are trying to determine the identity of this individual, not his record of substance abuse or not, not his medical condition, not his family's medical condition—many of the concerns that we are all terribly concerned about. They are just trying to find out who this individual is so that presumably, they can go and find him and question him, or find her and question her.

Mr. WEICH. Right. Let me say, Senator——

Senator REED. And you are saying that that would go across the line without some sort of court-approved search warrant?

Mr. WEICH. Right. But my point is that I think a search warrant would be issued in that case. I think it is appropriate. The reason why we believe the police should have to seek a search warrant is because there were many factual scenarios that are going to be a lot murkier. Let me pose one to you.

What is there is a crime scene, and somebody at the crime scene spilled blood, and that blood is type O-positive, and all the police know is that there was an African American male involved, and they want to find out which African American males have type O-positive blood, and they are going to ask hospitals that question. Well, that is a far more sweeping search.

Senator REED. And also—and I am not a law enforcement officer—probably a search that they would not conduct because it is so sweeping.

But the point here, I think—and this is what we are hearing from the Justice Department and I think we hear from the ACLU and others—you cannot think of an example where they would not have to get a search warrant, and they cannot think of an example where they would have to get a search warrant. That is a problem for us.

Mr. WEICH. I understand that, Senator. But in fairness, I really have to say that there are many cases where, because of the urgent need to prevent physical harm to somebody, the police will not need a search warrant. That is well-established in Fourth Amendment law.

Senator REED. We can agree with that, and in fact that is embodied in the Kennedy-Leahy legislation, and I think that point is a good one. But there are still these situations where you literally are looking for a suspect, you have good evidence that the person might be seeking medical treatment, and you do not care what kind of treatment he has or she has, what the prior medical history is, but you want to find that person just to question him. That is the area—that is one of those gray areas where I think we have got to come to trips in order to have a bill that will pass.

The other thing I should say, too, is that one of the reasons why I think the Justice Department is at this point less than forthcoming with suggestions is that I think they perceive there is a real concern that if language like "hot pursuit" got into the bill, it would be limited because the ACLU would go in and argue that, well, "hot pursuit" does not apply to this situation, and so on.

Mr. WEICH. Except that there is nothing unduly burdensome about the requirement that the police obtain a warrant. I think there may be a misperception that this is something which is going to require days of effort and litigation and motions back and forth.

Let me just, if I may, briefly describe what happens.

Senator REED. Yes. Can I ask a question before you do that? So your view is that it would be permissible now under the language in Kennedy-Leahy, for example, for the police to put out the proverbial all-points bulletin to all emergency rooms, asking not the identity, but have you treated a 5½-foot-tall middle-aged white guy for a bloody nose or something—that would be okay now, and then, to get the identity, they would have to get a warrant?

Mr. WEICH. That is correct. But if I may talk briefly about a search warrant——

Senator REED. Yes. Go ahead.

Mr. WEICH [continuing]. It really is not unduly burdensome. It is typically an ex parte proceeding, which means there is nobody on the other side; it is just the prosecutor going before a judge.

Where I practice as a prosecutor, in Manhattan, there was a judge who was literally on duty 24 hours a day. Arraignments in Manhattan go 24 hours a day. So if the police came to me, because I was the assistant district attorney on duty at that point, and said, "We need a search warrant on the following facts," and I made a legal judgment that there was probable cause on those facts, I would draft an affidavit for the police officer and literally walk the police officer down to the arraignments part on the first floor of my office building. The judge, who would be hearing a series of arraignments, would take a break between arraignments and hear us, either back in chambers or sometimes just at the bench, and he would swear in the police officer, listen to the facts, he might ask some questions to determine, to probe whether there really is probable cause on those facts, and if so, he would sign the warrant, and the officer was on his or her way to execute that warrant and search for the information.

It really is not an unduly burdensome requirement, and it serves a very important, fundamental constitutional principle, which is protecting everybody's privacy.

Senator REED. Thank you.

The CHAIRMAN. Even in the "hot pursuit" situation?

Mr. WEICH. Well, frankly, we do not see why "hot pursuit" would ever be relevant in the case of medical records. There are two different provisions at play here. The provision in the bills that says that if there is imminent danger of physical injury to somebody, you can obtain the records, that is there, and we have no problem with it.

"Hot pursuit" is a term of art in Fourth Amendment law which typically refers to, literally, the officers pursuing somebody who, if they were to stop to get a warrant, would lose the suspect; the suspect would evade arrest.

Now, if that is to be included in the bills, it might well address this situation. We think it should not be included because it potentially opens the door too much. But one way or another, you can find the words that create the common sense exceptions to the warrant requirements but still have the basic principle in place that in the routine case where nobody is running away, and nobody is bleeding, and a criminal is not about to commit another crime, that privacy is protected through a neutral magistrate evaluating where the probable cause is present.

The CHAIRMAN. When does an observation become a record? Suppose that in this case, the fellow has an injured hand, and they are going to go through records to find out whom they treated for an injured hand. Do you have to get a warrant for them to check the records and get the name of a person whom they treated?

Mr. WEICH. Just to clarify—at that point in your question, Mr. Chairman, are the police asking for the identity, or are they just asking the de-identified question, "is there such a person you have treated?"?

The CHAIRMAN. "Is there such a person you have treated?"

Mr. WEICH. As I read your bill, that is not protected health information, because it does not call for the identification of a person. So I do not think that is covered by the bill, and I do not think there is a lot of privacy interest in that plain vanilla question. So I think that is fine.

The CHAIRMAN. OK. I will leave it at that.

Professor Shapiro, could you respond just generally?

Ms. SHAPIRO. Yes, and this is, I have to say, outside the bounds of what the ABA policy would say, because the ABA policy does not speak so specifically to some of these issues. But from my own perspective, it seems like there is an opportunity here to work with the "hot pursuit" language in, for example, the Leahy bill and to balance the privacy interests versus the law enforcement needs and to, as Senator Reed suggested, acknowledge that by simply giving somebody's name and not the entire contents of his or her medical record in response to that initial police request so that they can pursue hotly this individual may be something that should be added to the hot pursuit provision.

The CHAIRMAN. Thank you both. It has been very helpful—or discouraging—I am not sure which—anyway, it has been enlightening, shall we say.

Thank you.

Appearing on our fourth panel to discuss the issue of authorization are 2 distinguished witnesses from the health care professions. First, I am delighted to welcome Ms. LaDonna Shedor, chief information officer and director of management information systems at Centra Health, a major health care provider in Lynchburg, VA. Ms. Shedor's career has involved the use of network computing to improve services and contain health care costs. Ms. Shedor, we appreciate your appearing before us today.

We also welcome Dr. Paul Appelbaum, testifying on behalf of the American Psychiatric Association, who is chairman of the Department of Psychiatry and director of the Law and Psychiatry Program at the University of Massachusetts Medical School in Worcester.

Dr. Appelbaum has long been interested in the area of confidentiality of medical information and patients' rights, having performed some of the few empirical studies on confidentiality of psychiatric records. We welcome you. Senator Kennedy apologized for not being able to be here, but as he indicated, there are other committees that are also trying to get some work done today, and he is on two important committees in that regard.

Ms. Shedor, please proceed.

STATEMENTS OF LADONNA SHEDOR, CHIEF INFORMATION OFFICER AND DIRECTOR OF MANAGEMENT INFORMATION SYSTEMS, CENTRA HEALTH, LYNCHBURG, VA, ON BEHALF OF THE HEALTHCARE LEADERSHIP COUNCIL; AND DR. PAUL APPELBAUM, CHAIRMAN, DEPARTMENT OF PSYCHIATRY, AND DIRECTOR, LAW AND PSYCHIATRY PROGRAM, UNIVERSITY OF MASSACHUSETTS MEDICAL SCHOOL, WORCESTER, MA, ON BEHALF OF THE AMERICAN PSYCHIATRIC ASSOCIATION

Ms. SHEDOR. Thank you. Good morning, Mr. Chairman and members of the committee. I hope I can share the kinder, gentler side of health care—the actual delivery in a community environment.

As you noted, I am the chief executive officer at Centra Health, and we are a not-for-profit health care provider in Lynchburg, VA. I am here today on behalf of the Healthcare Leadership Council, which represents the leaders and innovators of the health care industry from various sectors.

As the CIO at Centra Health, I am acutely aware of the power of patient information. It has the potential to dramatically improve the quality of the health care that we can deliver. It also has the potential to be harmful if it is misused.

Maintaining the trust of our patients by ensuring the responsible use of medical information is a fundamental cornerstone of our practice. We fulfill this promise daily, establishing the trust between our patients and our caregivers, and this is prevalent throughout our practices.

The Healthcare Coalition has been leading a broad effort in support of Federal legislation which largely mirrors the Centra Health philosophy—uniform standards are critical, and these will provide strong protections for patient health information while recognizing that the reality of health care delivery today is that it is driven by information.

This crucial ye delicate balance is recognized at Centra Health, and it is this very balance that the committee's efforts must achieve if it is to enact new law that demands greater accountability for how information is safeguarded, disclosed and used, but that also facilitates the responsible and appropriate use of patient information to fulfill our mission of providing better health care services to our community.

To enact Federal legislation which achieves the twin goals of patient confidentiality and enhanced quality requires you to develop a system of accountability and responsibility. But to work in the real world, standards must provide for flexibility—flexibility to design the systems and to implement policies which work in the particular environment for which that information is stored and used.

Centra Health has invested several millions of dollars in its electronic medical records and its security system, but the Central Health method may not be appropriate in other communities where there are larger populations or more diverse providers. Federal legislation must address the use of patient information by all the players in the health care delivery system. All of the standards that Congress develops must work for all of the health care entities.

At Centra Health, we boast a single information system that provides for about 250,000 lives. We have a significant amount of patient information already on line. We have a fully secured environment electronically, and we are expanding our capability for electronic medical records to enable our caregivers to access years of demographic information, medical results, medical histories and other critical information.

Our approach has been successful in our small community. It grants access to information based on need-to-know policies. We maintain an audit trail of all electronic access, searchable by medical record number, by user i.d., by location and by time.

All of these rules and security tactics are bolstered through very strict enforcement, including a policy of using good judgment which can and, I add, has resulted in termination of employees.

We believe that the appropriate way to handle authorization is to establish a mechanism whereby health care plans obtain a single authorization. This consolidated authorization approach is taken in the Bennett bill and to some extent in the Jeffords-Dodd bill. These bills allow health care plans to secure a single authorization at the time of enrollment for the disclosure and use of patient information for "treatment," "payment" and "health care operations"—terms that I understand are carefully defined in the bill.

Treatment and payment are well-understood functions. Health care operations, however, are less understood but equally important—services and functions fundamental to the ongoing and daily management and operation of the delivery system and the benefits contracts.

Conversely, we strongly oppose "multiple authorization" schemes that would require separate authorization from an individual each time medical information is accessed. Such a requirement each time even a subset of our daily, just over 850,000 electronic transactions, occurs would dramatically interfere with our ability to provide health care.

We strongly support consolidated authorization mechanisms, but we oppose proposals that would extend this approach to treatment and payment only. We are on the verge of using electronic information in a way that can change how we understand medical events. To require separate authorizations would dramatically impact that.

For instance, it makes no sense to use the information that we have available to treat an asthma attack but prevent that same information from helping that person become involved in an asthma management program and thus prevent another attack.

Finally, we approach the overall approach taken by Senator Bennett's legislation, as it most effectively establishes a workable yet balanced systematic approach to protecting patient confidentiality. It would create accountability by 1) requiring that patient information be safeguarded; 2) drawing clear and uniform boundaries around how patient information can be disclosed and used; 3) providing strong incentives to use nonidentifiable information where possible, and 4) establishing tough penalties for violating those requirements.

In conclusion, I want to reiterate the importance of your effort and the magnitude of what you are taking on. It is important to meet the August deadline imposed on Congress for action. I hope

this committee will build on these principles outlined in my testimony and pass legislation that strikes a balance that we all believe is necessary.

I thank you for considering my input.

The CHAIRMAN. Thank you.

[The prepared statement of Ms. Shedor follows:]

PREPARED STATEMENT OF LADONNA SHEDOR

Good morning, Mr. Chairman and Members of the Committee. My name is LaDonna Shedor and I am the Chief Information Officer (CIO) of Centra Health, a not-for-profit healthcare provider in Lynchburg, Virginia, comprised of a two-hospital campus, a home health care service, and a long term care facility. We also support 9 clinics and practices, two professional buildings, Lynchburg Family Practice and Residency Program, and a free clinic, and are a 50% partner in Piedmont Community Health Plan. Centra Health is a member of VHA, a nationwide network of more than 1,800 leading community-owned health care organizations and their physicians. The VHA network comprises 24 percent of the nation's community hospitals. Centra is also a member of the American Hospital Association.

I am here today testifying on behalf of the Healthcare Leadership Council (HLC), which is a Washington, D.C.-based trade association which represents the leaders and innovators in the health care industry from all its various sectors, including hospitals, health plans, physicians, and pharmaceutical, biotech and device manufacturers.

Thank you for this opportunity to testify regarding the most important topic of patient confidentiality. As Chief Information Officer at Centra Health, I am acutely aware of the power of patient information, both from its potential to dramatically advance the quality of health care services we deliver to our patient population as well as its potential to be harmful if abused or misused in any way.

As a result of this powerful duality, Centra Health has invested significant resources—both time and money—in developing information systems and policies which provide strong protections for the patient information we use daily, as well as state-of-the-art applications of this information to enhance quality and affordability of services. Maintaining the confidence and trust of our patients by ensuring the responsible and confidential use of their medical information is a fundamental cornerstone of our practice at Centra Health. We fulfill this promise today and every day through our commitment to and investment in security, and our policies regarding use and access.

As you are aware, the HLC has been leading a broad coalition effort in Washington in support of federal legislation which mirrors the Centra Health philosophy—federal, uniform standards that provide strong protections for patient health information, but that also recognize the reality that our 21st Century health care delivery system is driven by information. Simply put, access to information directly results in improved patient care. Ease of access to patient information directly results in greater utilization of such information, and of course, more utilization of the information means there exists the greater potential for abuse.

This crucial yet delicate balance is recognized at Centra Health, and is the very balance that this Committee's effort must achieve if it is to successfully enact new law that demands greater accountability for how information is safeguarded, disclosed and used, but that also facilitates the responsible and appropriate use of the patient information to fulfill our mission of providing better, higher quality, more responsive health care services. Far too often, I hear that we can only guarantee patient confidentiality by limiting through onerous authorization requirements, or even eliminating access to patient information, or that quality health care can be achieved only by sacrificing confidentiality principles. In fact, neither premise is true.

However, to enact federal legislation which achieves the twin goals of patient confidentiality and enhanced health care quality requires you to develop a system of accountability and responsibility. But to work in the real world, of standards and accountability must provide for flexibility—flexibility to design the systems and to implement policies which work in the particular environment in which the patient information is stored and used. In addition, any authorization processes established through federal legislation must be workable and ensure that information is readily available and accessible for activities that are vital to the on-going delivery of high quality health care services and items.

For example, Centra Health has invested several millions of dollars in its electronic record keeping and security system, but the Centra Health method may not

be appropriate for a hospital system serving a larger population, or for a highly integrated health plan which has partnerships with numerous hospital systems, physician group practices and employer sponsors of health care benefits.

Furthermore, federal patient confidentiality legislation must address the use of patient information by all of the players in our integrated health care delivery system, meaning that all, of the standards Congress develops and implements must work for all different shapes and sizes of hospitals, health plans, and other components of our health care system.

At Centra Health, we boast a single information system for an area population of approximately 250,000, with a significant amount of patient information provided on-line. Our system experiences approximately 850,000 transactions per day, as fifty percent of our local physician offices access CentraNet. We have a fully secured environment and are expanding our capability for a longitudinal electronic medical record which will enable us to access years of demographic information, medical results, medical histories and other critical information.

Our approach has been successful in our small community. We have worked diligently to raise awareness through formal agreements with our employees, the physicians with whom we work and their staff. Our system grants access to information based on role, location and need-to know policies. In addition, we maintain an audit trail of all access, searchable by medical record number, user, location and time. All of these rules and security tactics are bolstered through strict enforcement, including a Policy of using "good judgment" which can, and has, resulted termination of employment.

It is important that federal legislation be flexible enough to allow private sector to design its own systems and policies so they are workable in a variety of settings.

As mentioned earlier, it is also critically important that proposals requiring patient authorization for use of information be workable and allow such information to be used for vital health care delivery activities.

We believe the appropriate way to handle the sensitive issue of authorization is to establish a mechanism whereby health plans are able to obtain a single authorization up front, which then enables the use and disclosure of patient information for specific purposes related to health care delivery, including all of the activities we provide as a care giver. This "consolidated authorization" approach is taken in Senator Bennett's (R-UT) "Medical Information Protection Act of 1999" and, to some extent, Senator Jefford's (R-VT) and Dodd's (D-CT) "Health Care Personal Information Act" (S. 578). Specifically, these bills allow health plans to secure a single authorization at the time of enrollment in the plan for the disclosure and use of patient information for "treatment," "payment," and "health care operations"—terms carefully defined in the bill. Treatment and payment are well understood functions. Health care operations include the behind the scenes—yet equally important—services and functions fundamental to the ongoing and daily management and operation of the delivery system and the benefits contracts. Such services include coordinating patient care, risk assessment, case management, quality assessment, accreditation, credentialing, and utilization review.

Conversely, we strongly oppose "multiple authorization" schemes that would require that a separate authorization be obtained from the individual each and every time medical information is accessed. Such a multiple authorization scheme would unnecessarily interfere with the ability of systems such as Centra Health to provide effective treatment, to conduct important research activities and to ensure higher quality of care.

As mentioned, our system at Centra Health experiences approximately 850,000 transactions per day. A requirement that a separate patient authorization be secured each time even a small subset of these transactions is attempted would interfere with our ability to provide the health care we deliver to thousands of patients. It would also be met with the disapproval of the vast majority of our patients who already chafe at the volume of paperwork required in our system.

In the rare cases where states have enacted a multiple authorization requirement, the results have been predictable. Most recently, the State of Maine suspended their "Act to Provide for the Confidentiality of Health Care Information" just 14 days after it took effect in large part because chaos that ensued due to cumbersome multiple authorization requirements.

While we strongly support consolidated authorization mechanisms, we oppose proposals that would extend this approach to treatment and payment only, requiring separate authorizations for the use of information to conduct crucial health care operations. This is the approach taken in the "Medical Information Privacy and Security Act," (S. 573). Such a scheme is unworkable in our highly integrated health care delivery system.

For instance, it makes no sense to allow the use of information to treat an acute asthma attack, while requiring a separate authorization to use the same information to prevent the attack by effectively coordinating care for the patient through an asthma management program.

Importantly, the authorization mechanism established under the Bennett bill limits the use of information to specific healthcare-related activities. Authorization for the use of information beyond purposes of treatment, payment and health care operations would require a separate and specific authorization by the patient. As such, egregious abuses of health information would be prohibited.

In addition to Senator Bennett's bill's approach to authorization procedures, we support the overall approach taken by Senator Bennett's legislation as it most effectively establishes a workable and balanced systemic approach to protecting confidentiality. Very simply, it will create accountability by: (1) requiring that patient information be safeguarded; (2) drawing clear, uniform, and understandable boundaries around how patient information can be disclosed and used; (3) providing strong incentives to use non-identifiable information where possible; and, (4) establishing tough penalties for violating these requirements. This is preferable to other approaches which attempt to minimize possible abuse by micro-managing information flow to the ultimate detriment of the system and to patients.

In conclusion, I want to reiterate the importance of your effort and the need to meet the August deadline imposed on Congress for action. I hope this Committee will build on these principles outlined in my testimony and pass legislation that strikes the balance we all believe necessary.

The CHAIRMAN. Dr. Appelbaum.

Dr. APPELBAUM. Mr. Chairman, I am Paul Appelbaum, M.D., testifying on behalf of the American Psychiatric Association, a medical specialty society representing more than 40,000 psychiatric physicians nationwide. I serve the APA as its vice president-elect, and I am also, as you noted, professor and chair of the Department of Psychiatry at the University of Massachusetts Medical School. I think I am the only physician and probably the only person treating patients who is testifying before you here today, and I would like to thank you for this opportunity.

Mr. Chairman, we greatly appreciate your commitment to passing medical records privacy legislation and note that your bill contains valuable provisions that will enhance patient privacy. We would also like to applaud Senator Kennedy for the legislation he has introduced with Senator Leahy, which will provide a very high level of confidentiality protections for patients.

Patient privacy is a valuable right in and of itself and requires protection so that patients will be willing to seek needed medical care and that the care that is provided will be of the highest quality.

It is not my intention here today to provide an analysis of each of the bills before the committee. Rather, I would like to comment on the general principles that we believe should guide whatever legislation is adopted and then note several implications of those principles.

Three principles should govern those sections of the legislation concerning authorization and consent for disclosure. First, patients themselves should decide whether or not personal health information is disclosed. This has been our historic standard, embodied in common law and professional practice. Those who would alter this traditional procedure have failed to justify such a radical change.

Second, identifiable personal health information should be released only when de-identified data are inadequate for the purpose at hand. The burden should be on the person seeking access to the information to prove the necessity of using identifiable data.

Third, even when consent has been obtained, disclosure should be limited to the least amount of personal health information necessary for the purpose at hand. The bill introduced by Senator Kennedy and Senator Leahy incorporates these principles in the authorization sections and indeed throughout the legislation. Of all the proposals before the Congress, the Leahy-Kennedy bill will clearly provide the highest level of privacy protection for patients, thus improving the quality of care enjoyed by Americans. We also believe that these and other needed principles can be incorporated into the framework established in the legislation introduced by you and Senator Dodd.

These principles have implications for some of the major policy questions regarding authorization of disclosure. For patients to retain meaningful control over personal health information, prospective consent for routine disclosure should be limited to information needed for treatment and payment purposes. Other health care operations can usually be accomplished with de-identified data. And patients should be informed before disclosures are made so that they have a reasonable opportunity to withdraw consent if they so desire.

Patients' ability to maintain their privacy also requires that in cases where patients pay expenses out-of-pocket, patients must not be compelled to have their information used for purposes beyond treatment of their medical condition. We support the right of self-pay patients to maintain the maximum level of privacy by limiting disclosures of their personal information to their immediate treatment team.

Patients should also retain the right to limit access to sensitive information in their medical records so that it is not available to everyone with whom they may come into contact in an integrated health care system. In fact, it is perfectly understandable that a patient may not want his dermatologist, who is his spouse's tennis partner, to know about his mental health issues, alcohol abuse, or sexual history. Such privacy protections are particularly important in tightly knit communities or in rural areas.

When patients act to protect their interests by withholding consent for disclosure for any of these reasons, health plans, facilities or providers should not be able to force patients to consent to disclosures by denying them care, terminating them from their plan, or denying payment for a claim. No compelling case for establishing such a coercive consent mechanism has been made.

There are numerous other examples that can be used to document how and why a high level of protection should be applied to medical records information. Indeed, as a psychiatric physician, it is particularly easy for me to point out the importance of the legislation before the committee. Patients often refrain from entering psychiatric treatment because of concerns about confidentiality. Without the very highest level of confidentiality, patients receiving mental health services will be less likely to enter treatment and less likely to remain in treatment. And I might note that this extends not simply to mental health treatment but to other populations with particular concerns about privacy, for example, adolescents. We have several studies that demonstrate that once frightened by the prospect that confidentiality of their medical records

will not be maintained, adolescents are highly unlikely to seek treatment even for conditions such as sexually-transmitted diseases for which treatment is essential.

For these and other reasons specifically related to mental health treatment, the U.S. Supreme Court recognized the special status of mental health information in its 1996 Jaffe v. Redmond decision. I urge you and the other members of this committee not only to protect the letter of this decision but indeed to protect its spirit by including appropriate provisions in this legislation.

We thank you for this opportunity to testify, and we look forward to working with the committee on these important issues.

[The prepared statement of Dr. Appelbaum follows:]

PREPARED STATEMENT OF DR. APPELBAUM

Introduction

Mr. Chairman, I am Paul Appelbaum, MD, testifying on behalf of the American Psychiatric Association (APA), a medical specialty society, representing more than 40,000 psychiatric physicians nationwide. I serve the APA as its Vice-President Elect and Chair of its Ethics Appeals Board, and I am also Professor and Chair of the Department of Psychiatry at the University of Massachusetts Medical School where I see patients on a regular basis. I would like to thank Chairman Jeffords, Senator Kennedy, and members of the Committee for the opportunity to testify today.

Mr. Chairman we greatly appreciate your commitment to passing medical records privacy legislation and note your bill contains valuable provisions that will enhance patient privacy. We also would like to applaud Senator Kennedy for the legislation he has introduced with Senator Patrick Leahy (D-VT), which will provide a very high level of confidentiality for patients. Strengthening patient privacy and the confidentiality of the doctor-patient relationship—key foundations of our health care system—is critically important. Patient privacy is a valuable right in and of itself, and it is also necessary to insure that patients will be willing to seek needed medical care and that the care that is provided will be of the highest quality possible.

In recent years, as changes in technology and health care delivery have outpaced the statutory, common law, and other protections that traditionally have ensured patient confidentiality, the level of confidentiality enjoyed by patients has eroded dramatically. I greatly appreciate your efforts to seize this valuable opportunity to protect and restore needed confidentiality protections.

The Need for Federal Legislation

I believe medical records confidentiality is one of the most important issues that will come before the HELP Committee this year. Our ability to find a new job or earn a promotion, our ability to obtain insurance, our family and social relationships, the quality of health care, and medical research breakthroughs can all be enhanced or tragically jeopardized by medical records confidentiality legislation. Our medical record, when it relates to conditions as varied as high blood pressure, communicable diseases, Alzheimer's disease, mental illness and substance abuse, domestic violence, sexual assault information, terminal illnesses, HIV/AIDS, cancer, eating disorders, sexual function and reproductive health issues, as well as other conditions, is highly sensitive. But whether or not we are affected by these illnesses, we are all affected by medical records privacy issues. Today's comprehensive medical assessments and wellness questionnaires can also contain extensive medical, personal and financial information. The forms can contain questions about patients' sexual behavior, social relationships, state of mind, and psychiatric status—even if patients are not receiving medical treatment relating to these issues.

The need for legislation is compelling. In 1996, a federally appointed panel of experts, the National Committee on Vital and Health Statistics stated that our country faces a "health privacy crisis." And broad bipartisan support exists for action on this issue. From Phyllis Schafly's concern over the "stealth assault on medical records" and civil libertarians' desire to insure that the Fourth Amendment applies to police efforts to obtain medical records, to bipartisan concern that led to a suspension in any implementation of a national patient identifier, Americans of all political persuasions want to keep their personal medical information confidential. We hope that these strong bipartisan sentiments can be used to overcome any differences and enact into law federal medical records legislation meaningfully protective of patient privacy.

Confidentiality is a Requirement for High Quality Medical Care

Common sense, the experience of physicians and patients and research data all show that privacy is a critical component of quality health care. The sad fact is that the health care system has, on occasion, not earned the trust of patients, and many patients do not trust the system to keep their information confidential. In many cases the result has been that physicians are not able to provide the best possible quality care and indeed to reach many individuals in need of care.

Some patients refrain from seeking medical care or will drop out of treatment in order to avoid any risk of disclosure. And some will simply not provide the full information necessary for successful treatment. At other times physicians are approached by patients who ask us not to include certain information in their medical record for fear that it will be indiscriminately used or disclosed. The result of all these behaviors resulting from patients' reasonable concerns is unfortunate. More patients do not receive needed care and medical records' data that we need for many purposes such as outcomes research is regrettably tainted in ways that we often cannot even measure.

The solution is not to take short cuts that will further deprive patients of their rights. Instead, we must enact into law meaningful medical records privacy legislation based on the voluntary informed consent of patients and reliance upon the fullest possible use of deidentified and aggregate patient data. In this way the full advantages of patient privacy as well as the benefits of new medical technology can be harnessed.

Informed, voluntary, and non-coerced patient consent before the use and disclosure of medical records should be the foundation of medical records confidentiality legislation. As a general principle we believe that the American Medical Association's position—that patient consent should be required for disclosure of information in the medical record with narrowly drawn and infrequent exceptions permitted for overriding public health purposes—is eminently reasonable.

The Leahy/Kennedy/Daschle bill and Chairman Jeffords' bill introduced with Senator Dodd to different degrees do contain important protections in the authorization provisions to insure that patient consent is informed, voluntary and non-coerced. And the bill introduced by Senator Robert Bennett (R-UT) does establish an authorization framework preserving the principle of consent before disclosure to which needed protections can be added.

It is not my intention to provide an analysis of each bill but rather, I would like to comment on general principles that we believe should guide whatever legislation is adopted by the Committee.

Three principles should govern those sections of the legislation concerning authorization and consent for disclosure. First, patients themselves should decide whether or not personal health information is disclosed. This has been our historic approach. In general, whatever problems may now exist with confidentiality of health information is derived from our failure to observe this principle. No one is in a better position than patients themselves to identify sensitive information and to determine to whom it ought not to be revealed. Those who would alter this traditional approach have failed to justify such a radical change. Second, identifiable personal health information should be released only when deidentified data are inadequate for the purpose at hand. The burden should be on the person seeking access to the information to prove the necessity of using identifiable data. Third, even when consent has been obtained, disclosure should be limited to the least amount of personal health information necessary for the purpose at hand. This is consistent with our recognition of the importance of protecting medical privacy.

These principles have implications for some of the major policy questions regarding authorization of disclosure. For patients to retain meaningful control over personal health information, prospective consent for routine disclosures should be limited to information needed for treatment and payment purposes. Other health care operations can usually be accomplished with deidentified data. With such a provision a strong incentive will exist for the use and further enhancement of technology to perform a wide array of administrative functions. If identifiable data is needed, separate consent could be obtained, as outlined in the Leahy/Kennedy/Daschle bill. Another option is to make modifications in Chairman Jefford's bill in order to insure that patients can meaningfully revoke consent particularly for administrative or "operations" purposes.

Patients' ability to maintain their privacy also requires that in cases where a patient pays for his own expenses out of pocket, the patient must not be compelled to have his information used for purposes beyond treatment of their medical condition. Frankly I believe such a provision is consistent with the principles of individual liberty, basic privacy, and good health care. If individuals enter into a private contract with a physician and pay for those medical services out of their own pocket,

it is difficult to understand why the government or a health plan should compel them to sign a form allowing their medical information to be broadly disclosed beyond the treatment team. The American Psychiatric Association has supported medical savings accounts and private contracting rights for Medicare beneficiaries in order to protect patient privacy and informed consent. For these and other reasons we support the right of self-pay patients to maintain their freedom and privacy through making basic choices about the use of their confidential information.

Patients should also retain the right to limit access to sensitive information so that it is not available to the thousands of nurses and doctors in an integrated health care system who are not involved in their care. In fact, it is perfectly understandable that a patient may not want their dermatologist, who is their spouses' tennis partner, to know about their mental health issues, alcohol abuse, or sexual history. Such privacy protections are particularly important in tightly knit rural areas where there are a small number of health care providers.

When patients act to protect their interests by withholding consent for disclosure for any of these reasons, health plans, facilities, or providers should not be able to force patients to consent to disclosures by denying them care, terminating them from their plan or denying payment for a claim. No compelling case for establishing such a coercive consent mechanism has been made.

In particular, the APA is also very concerned by the definition of "operations" in several of the proposals before the Senate. Each patient's authorization form must include provisions for the use and disclosure of medical records for "operations" purposes i.e. many purposes not directly related to treating a patient or performing payment or reimbursement functions. Some of the terms that are used in defining this term are quite vague and broad and could endanger patient privacy. Do we really want to permit patients to be terminated from their health care coverage because they don't want their personal records to be used for a largely commercial function that can be performed with aggregate data?

Millions and millions of Americans have great concern about the threat to confidentiality of their medical records due to employer access. Certainly many employers have an excellent record of protecting patient confidentiality, yet some employers are not so cautious. For this reason, we need a medical records privacy law that will protect all employees. Whether it is idle gossip by individuals with access to medical records, employer review of identifiable medical records data, or supervisors' inappropriate interest in the personal lives of their employees we must protect employees right to medical records privacy. Wouldn't most people want to decide if anyone in their company, not to mention their supervisor, would know if they obtained medical care from a psychiatrist, from a cardiologist, or from an oncologist? Wouldn't you want to decide if anyone would know about any reproductive health or fertility treatment or services you had used?

We and numerous other groups believe that the strongest possible explicit protections are needed in this area. Employers must not disclose personal health information to supervisors, and others who make employment and personnel decisions without a separate specific authorization. Otherwise, if it is part of a general and broad consolidated authorization—a form that a patient may sign only once in a decade when they enroll for medical coverage - employees will be signing away important rights without even knowing it.

The bill introduced by Senator Kennedy and Senator Leahy incorporates these principles in the authorization section, and other needed privacy protections are included throughout the bill. Of all the proposals before the Congress the Leahy-Kennedy bill will clearly provide the highest level of privacy protection for patients, thus improving the quality of care enjoyed by Americans. We also believe that these and other important principles can be incorporated into the framework established in the legislation introduced by Chairman Jeffords and Senator Dodd.

Federal and State Government Access to Private Medical Information

Given the sensitivity of the information contained in today's medical records we should remember that this legislation will also govern access to identifiable medical records by state and federal governments' health, law enforcement, and other agencies. One example of the type of broad government access to identifiable medical records information without the fully informed, voluntary consent of the patient that we must guard against is the OASIS comprehensive medical assessment developed for use by local home health care agencies by the Health Care Financing Administration (HCFA).

The assessment includes detailed information on patients' living arrangements, financial status, and mental health information (even if they are not being treated for such a condition). For example, information on all patients' ability to pay for rent and utilities, and any disruptive behavior or feelings of failure, must be included in this form. The agencies would be required as a condition of their participation

in Medicare to report the information collected including patient names to state and federal governments. Depending on the decisions made in the next several weeks by the Office of Management and Budget, much of this highly sensitive information would have to be transmitted to the federal and state governments, including information on non-Medicare patients and even patients who pay out of pocket for medical services. Such non-aggregate patient identifiable information should not routinely be reported to the state and federal governments.

The Special Sensitivity of Mental Health Information and the U.S. Supreme Court's Jaffe decision

There are numerous other examples that can be used to demonstrate how and why a high level of protection should be applied to medical records information. Indeed as a psychiatric physician it is particularly easy for me to point out the importance of the legislation before the Committee. It is also worth recognizing that the extent of mental illness is widespread. According to the World Health Organization mental illnesses account for four out of ten of the leading causes of disability.

Suffice it to say that patients often refrain from entering psychiatric treatment because of concerns about confidentiality. Not only do patients refrain from telling family members and close friends the information they share with their therapist but they may not even tell their family members that they are receiving treatment. In some cases if the information were disclosed to a spouse or an employer it might jeopardize their marriage or employment. But even the privacy protection afforded to psychotherapy notes has eroded so far in recent years that many psychiatrists and other mental health professionals have stopped taking notes or take only very abbreviated notes. Without the very highest level of confidentiality, patients receiving mental health services will be less likely to enter treatment and less likely to remain in treatment. Worse yet, if confidentiality is not protected, the treatment they receive may be less effective.

For these and other reasons the U.S. Supreme Court recognized the special status of mental health information in the 1996 Jaffe v. Redmond decision. The court held that "Effective psychotherapy depends upon an atmosphere of confidence and trust . . . disclosure of confidential communications made during counseling sessions may cause embarrassment or disgrace. For this reason the mere possibility of disclosure may impede the development of the confidential relationship necessary for successful treatment." I urge members of this committee not only to protect the letter of this decision but indeed to protect its spirit by including appropriate provisions in the legislation.

As physicians, we take an oath first stated by Hippocrates that "Whatsoever things I see or hear concerning the life of men, in my attendance on the sick . . . I will keep silence thereon, counting such things to be as sacred secrets." In order to make sure that doctor-patient confidentiality continues to protect patients in the new millennium, I strongly urge the Committee to provide the highest possible level of confidentiality in your legislation.

We thank you for this opportunity to testify, and we look forward to working with the Committee on these important issues.

The CHAIRMAN. Thank you very much, both of you, for excellent statements. We will be keeping in touch with you as we wind down toward the end of the next month.

Ms. Shedor, in your testimony, you discuss the need for flexibility in developing confidentiality standards. Do you believe it is possible to allow for flexibility while at the same time truly safeguarding information?

Ms. SHEDOR. Yes, I do. I think that most of the people in health care delivery are focused on the care of the patients, but that individual communities, the size of the entities involved, would dictate different applications.

The thing that confuses or confounds local health care delivery in my opinion is unclear guidelines. As care is shifting in different ways—for example, much care used to be delivered in the acute environment; now, much more is delivered on either end, either in clinics, physicians' offices, and home health on the other end—the continuity, the sharing of information across all those entities, which may or may not legally be part of the same group, is crucial. And if we require different signatures at each point along the way,

we will necessarily slow down the process; we may inhibit the free flow of information.

I really believe, having seen what happened in Centra Health, that individual communities will meet the goals if the goals are clearly defined. I think there is no question.

The CHAIRMAN. Ms. Shedor, while my bill and Senator Bennett's bill both allow for consolidation authorization, others may argue that patients may not want their information used for health plan operation activities. In your experience at Centra Health, do many patients request their medical information only to be used for certain purposes?

Ms. SHEDOR. I think that most individuals right now do not know to ask that question. They look to us to provide not only the care that they are requesting, but also to advise them on care they may require. It is important for us to be able to send out reminders to ensure that individuals follow up on their health care. As I understand it, some of the bills would limit that possibility, and I think it is important that we be able to do that—that we are able to do disease management—and that requires us to analyze all of this data.

The CHAIRMAN. Although I am sure it is rare that one of your employees violates the rules for disclosing information, can you describe your policy of good judgment by employees and how it is enforced?

Ms. SHEDOR. Our policies require that there be review of any breach of confidentiality by the related group. For example, if there is a breach by an employee, the employee human resources individuals are involved; if there is a breach by the professionals, the professional committees are involved. In order of event, if there is a complaint or a sense of a breach, we pull from the electronic records the audit trail of the relevant employee or the relevant record; we examine that, and we determine whether there was a legitimate reason for that individual to be accessing that data in the manner that they were. If we can determine no legitimate use, that person is counseled and terminated if appropriate. And it has happened, as I said.

The CHAIRMAN. We anticipate the eventual utilization of all our modern technology to the best medical advantage, and we are able to benefit from international communications about outcomes analysis. Does this bill in any way impede good outcomes analysis, so that we can use information which does not identify individual patients?

Ms. SHEDOR. That is a really tough question. To do good outcomes studies—and we are all struggling with what the definition of "good outcomes studies" is in an electronic world—you need to have access to all of the relevant data. For example, I am a diabetic, and I know that my instinct is not to report my glucose readings when I have not been compliant. If those readings during that period of time are excluded from the study, you get skewed results.

I think it is important that if we are going to do disease management in this country that we include all the relevant data and truly detach that from the patient identification. It is not necessary to have individual patient identification, which I think is the issue here——

The CHAIRMAN. Yes.

Ms. SHEDOR [continuing]. For outcomes. On the other hand, I expect and fully believe that health care plans should help individual patients manage their disease, and to do that, we have to have a continuous picture of what is going on with that patient. And that does require the boundaries to be crossed within an individual delivery system, within a State, and interstate. We are not real close to the border, but we have patients who go into North Carolina, for example, to Duke University, and we would want to be able to really ship their records as needed to their health care providers.

Dr. APPELBAUM. Senator, may I comment on that?

The CHAIRMAN. Yes.

Dr. APPELBAUM. "Disease management" is a new catch phrase or term of art that is being used in health care today, and it means different things to different people, but in one of its guises, what it means is that health care organizations or managed care plans contract with outside entities to oversee the care for particular conditions that their patients are receiving. "Overseeing" may mean intensive efforts to follow up with patients, to phone them, to make sure they are taking medications, to suggest additional things that they may do to change their lifestyle, to encourage them to come to appointments—things which in many respects may be good but are in another respect actually highly intrusive and a very different way from the way we have practiced medicine in the past. And for the treating entity to turn over patient care information to this third party that is conducting these disease management protocols means a serious breach in the traditional walls governing patient medical record information confidentiality.

Should patients desire such disease management, should someone being treated for diabetes find that to be helpful to them, I think we would say patients should have the right to consent to it. But since many patients will react otherwise, we believe strongly that patients should be given the option as to whether their information crosses those boundaries, is turned over to a third party entity and is used for those purposes.

The CHAIRMAN. So when you get a general release from a patient that says yes, you may disclose my record, when does that agreement cease to be valid? In other words, suppose someone has one disease, and subsequently contracts another. Does that initial release, permitting disclosure, still apply?

Dr. APPELBAUM. This is where we have some concerns about the general authorization procedures that are actually in all three of the bills under consideration. Clearly, there is some need for authorization for disclosure for payment purposes and for ordinary use in treatment settings.

Our concern is that these consents are obtained prospectively, at the time someone signs up for insurance or enters a health plan. At that point, one may have no idea of the kind of information that will ultimately be disclosed. How one deals with that could occur in several ways, but if there is going to be a blanket, up-front authorization process, we think it is very important for patients to have some meaningful control over the release of information even under that process, which means they need to be informed prior to subsequent disclosure of information and be given the opportunity

to object to that disclosure. So if I signed up and I said I thought I was healthy, and I said you could release whatever information you want, because I could not conceive of information that might be embarrassing to me, and I subsequently contracted a sexually-transmitted disease, the disclosure of which I did not want to occur to my family physician who is also my close friend, I would then be given the option to preclude that information from being released.

We also support provisions that would allow such information to be sequestered within medical records and released only under particular circumstances.

The CHAIRMAN. This is a most difficult area to me as we take a look at the broad picture of how we can better medical science and get all the information we need on outcomes. But the most important concern is in your area of psychiatry, and it is incredibly important that we give confidence to people that their personal psychiatric information is not being misused.

I just want to let you know that I am very deeply interested in all of these issues, and I hope we can look to you to guide us next month as we go down toward the finish line.

Thank you both very much for your efforts, and we look forward to working with you.

Dr. APPELBAUM. Thank you, Senator.

Ms. SHEDOR. Thank you.

The CHAIRMAN. Our final panel of witnesses today will discuss the topic of preemption. First, I am happy to welcome Dr. John G. Curd, vice president of clinical development at Genentech, Inc., in San Francisco. Before joining Genentech, he headed the Division of Rheumatology and was vice chairman of the Department of Medicine at Scripps Clinic and Research Foundation in La Jolla, CA. Dr. Curd is a fellow of the American Academy of Allergy and the American Rheumatism Association.

Dr. Curd, welcome, and please proceed.

STATEMENTS OF DR. JOHN G. CURD, VICE PRESIDENT OF CLINICAL DEVELOPMENT, GENENTECH, INCORPORATED, SAN FRANCISCO, CA; AND CHRIS KOYANAGI, DIRECTOR OF LEGISLATIVE POLICY, JUDGE DAVID L. BAZELON CENTER FOR MENTAL HEALTH LAW, WASHINGTON, DC, ON BEHALF OF THE CONSUMER COALITION FOR HEALTH PRIVACY

Dr. CURD. Thank you, Mr. Chairman.

Mr. Chairman, ladies and gentlemen, this is really a critical issue that we are talking about today. Confidentiality of patient medical information is going to affect patients individually and the society's health care, and you really have to deal with that balance.

When I think of myself, I graduated from medical school 30 years ago, I have done research for the NIH, I understand clinical research and NIH guidelines, I practiced medicine for 10 to 15 years, I was president of the medical staff for a hospital that dealt with the regulations that you all have put forth to us, and in the last 7 to 10 years, I have done drug development.

Among the things I am most proud of, I have participated in the development of Pulmozyme for cystic fibrosis, the first drug for cystic fibrosis; I helped to develop a drug for nonHodgkins lymphoma,

again the first; and most recently, I worked on Herceptin for women with breast cancer. So I have had a broad-based experience both with patients, their medical information and the use of that information for research.

When I think of my own personal experience as well as that of many others in academics and in research, we really need to understand appropriate access and use of patient medical information. It is critical that you enact strong, uniform Federal standards designed both to safeguard on one hand the confidentiality of patient information and to limit its use to the activities that are appropriate and necessary for the daily functioning of our dynamic health care system.

Probably every person in this room, certainly every person's family, has benefited from medical research that has been done in the last five or six decades, and we need to look forward to what is going to happen in the next five or six decades. The medical research community has to have uniform standards for the performance of clinical and medical investigations. If we think of the legislation that is going to protect privacy and confidentiality of patients, it has got to protect them from abuse. But we need to make absolutely sure that that legislation does not build up barriers so that medical researchers cannot get access to the information that they need to do further medical research. We do not want to slow and impede medical research. We do not want to do ultimately harm to the generations of people who are depending on us.

If we think about it, one principle of medicine is to do no harm; so as I have practiced medicine, I have always had in my mind do not injure the patient. That is relevant to what you are doing here. Your legislation is important to protect the patient, but it should not do harm.

So if we look forward and we just think about some of the things that are practically happening today, one of the best places in the country for patient information and population research has been the Mayo Clinic. Founded in 1907, from the very beginning, the founders of the Mayo Clinic had the foresight to say we need to look critically at our own experience. They did that both in the natural history of diseases and the outcomes of their patients for both surgical and medical interventions. And if we think about it, they have also been a leader. At the time computer were first invented, the Mayo Clinic was indexing and using patient population information to provide critical data about population and diseases in the United States, and they have continued to do that. They are now leaders in the computerized medical record, and they have institutions in Florida, Arizona and Minnesota.

We heard today, actually, that Minnesota has passed a law which has made it practically more difficult for the Mayo Clinic to conduct broad, population-based research by requiring specific patient authorization for use of patient data. That law started in 1997. I have brought a paper that was published in 1999, in the last few months, and what it shows is that compared to 1997, when 3 percent of patients refused to have their medical information used for research, in 1999, that very same patient population, 30 percent of patients refused to respond to the first questionnaire asking for permission. After they did it three additional times over

3 months, 20 percent of the same patients never responded. Now, of that 20 percent, only 4 percent said you cannot use my information. The other 16 percent just did not respond; they were noncompliant.

Now, if you think about what that means in a statistical sense, if you have a population with only 80 percent of the people responding, you have 20 percent of the people not responding, and in a biostatistical sense, it makes any conclusions that you will draw from that population much less valuable, much less high-quality, and perhaps even irrelevant.

Imagine the situation where some of those patients have died, and you can never get response. How are we going to get information on critical diseases like cancer and AIDS and heart disease, where people are actually dying and cannot provide consent for their information?

If I stop, then, and think about another place—let us compare drug development in the United States to drug development in Europe. Almost every pharmaceutical company likes to do drug research in the United States. Why? Because we have relatively uniform FDA standards that are applied by institutions, researchers and hospitals across the United States. Compare that with watt goes on in Europe, where you have Spain, the United Kingdom, France, Germany and a variety of other countries, each with their own regulatory agency, each with their own set of laws. And what happens in fact is that it is practically much more difficult to do research in Europe.

I do not want the United States, with a lot of State laws, to become like Europe. If that happens, as a drug developer, I am going to look for a better place to spend my time and money, and ultimately, what that will do is take away some of the leadership that has happened in the United States in terms of drug development.

There was a discussion by the previous presenters about outcomes research. One of the things that I am actually most proud of is the National Registry for Myocardial Infarction that has been sponsored by Genentech. It is in 1,500 hospitals in the United States. A recent article showed that in fact if you live in a different region of the country, you are less likely to get treatment for your heart attack. It also showed that in fact, if you are a woman, particularly if you are an older woman, you have about a 25 percent reduced likelihood of getting effective, accurate diagnosis and treatment.

Having information across the country is what is going to allow us to deal with outcomes research and improve the quality of medical care, which will translate into savings in terms of the health care delivery system and benefits for our patients.

The last example I want to talk about is genetics and genomics. If you think about it, one thing that is really powerful about our technology is that we are beginning to understand those principles which develop in the patient that affect drug metabolism. The FDA now requires us in fact to do subpopulation pharmacokinetic analysis for drug development—older people, younger people, people with kidney function, Hispanics, blacks.

Why is that? Because safety and efficacy depend upon your genetic and racial background, and the FDA already requires that. So

now we are getting into the situation where we are understanding the genetic basis of drug interaction, safety and efficacy, and we are going to decide to exclude that information from use both in the treatment of patients and understanding how research could relate to drug development. This would be a bad thing.

To put that in perspective, in the 1970's, I was actually told that we should exclude women and children from drug studies. In fact, my IRB at Scripps Clinic excluded women and children because we wanted to "protect" them. The outcome of that was that we had almost no data on the people we protected.

Now, when the drugs were approved based on male studies, they were used in women and children, just the same as they were used in men, in the absence of data.

We do not want to have the unintended consequences of protecting people and then have them subjected to potential risk and harm because we have protected them.

Now, we have diverse laws governing patient confidentiality potentially developing in every State. This would require that people like myself have tailored programs to do research in every State. The variability, the diversity in different States will create a level of absolutely unnecessary complexity.

To address the complexity, researchers will need to spend more time and money to accomplish the research goals. The consequences will be to increase the cost of research, reduce the number of investigations that are done, and if you think about it, smaller numbers of more expensive studies are not in the best interest of patients or of the country.

If I put this in the context of where we are now in dealing with the legislation, the point I want to make is that uniformity provisions in the legislation are really critical, and for that reason, I personally favor the legislation that was introduced yesterday by Senator Bennett. Senator Bennett's bill provides very thorough preemption of State law, it create a uniform, predictable environment for the research community, it replaces current law with a rational, comprehensive program of Federal safeguards, responsibilities, limits and penalties.

To date, this is the only legislative proposal that would effectively address the concerns I descried earlier such as those at the Mayo Clinic. It does not sacrifice any of the protections provided to patients.

Conversely, proposals by Senators Kennedy and Leahy and by yourself and Senator Dodd could potentially undermine our ability to conduct broad, inclusive population-based research and could subject us to a new Federal standard as well as several conflict State laws.

Your committee has been a vital partner in assuring a stable, fruitful environment for biomedical research, as illustrated by your recent efforts on the Food and Drug Administration Modernization Act. Please understand that the ultimate impact of this issue is no different. It is directly related to innovation and research.

Be assured that we at Genentech and in the industry share your commitment to protecting and safeguarding patient information. After all, patients are our business. Also understand, though, that information is the life blood of research, and it is necessary for us

to have this information in order to basically evolve the health care delivery system and improve quality.

Thank you again, Mr. Chairman, for providing us this opportunity to address you and the committee.

The CHAIRMAN. Thank you.

[The prepared statement of Dr. Curd follows:]

PREPARED STATEMENT OF JOHN CURD, M.D.

Good morning, Mr. Chairman, and Members of the Committee. Thank you for the opportunity to testify before you today regarding this most important issue of the confidentiality of patient medical information. My name is John Curd, and I am Vice President of Clinical Development for Genentech, Inc., a San Francisco, California-based biotechnology company. Genentech, Inc. is a pioneer in the biotechnology field, responsible for the development of several breakthrough, life-saving biological products, including Pulmozyme for Cystic Fibrosis; Activase for cardiac disease; Rituxan, for non-Hodgkins lymphoma; and most recently, Herceptin for metastatic breast cancer.

Genentech, Inc. is an active member of the Pharmaceutical Research and Manufacturers of America (PhRMA), the Biotechnology Industry Organization (BIO) and the Healthcare Leadership Council (HLC). We have been working closely with these organizations and numerous other coalition partners through the HLC in support of enactment of strong, uniform federal standards designed to safeguard the confidentiality of patient health information and limit its use to activities which are appropriate and necessary to the daily functioning of our dynamic health care delivery system, including the use of information for biomedical research.

Throughout this effort, however, we have grown to realize that while such federal standards are needed to help assuage concerns over the abuse of patient health information and facilitate patient confidence in the system, it is equally critical that new federal law recognize that patient information is the foundation of our growing effort to enhance the quality of health care we deliver through accountability, outcomes analysis and medical research. Any failure to strike this delicate balance could have the dramatic and unintended consequence of stifling innovation and limiting the ability of companies like Genentech, Inc. to effectively continue its mission and pursuit of drug therapies for unmet medical needs. In addition, any new federal standards must create a single, uniform system of safeguards, accountability and penalties by which the research community must abide by preempting the increasing patchwork of state law which is working to minimize our ability to conduct research effectively and affordable.

I understand that this is the last in a series of hearings on this subject and you have no doubt heard from all the various sectors of the health care industry affected by the debate. Allow me to reiterate, however, the importance and saliency of your decisions to the biomedical research community and to the patients who suffer from the illnesses we study. While we at Genentech, Inc. are firmly committed to protecting the confidentiality of the patient information we review and use each minute of each day, our ability to hypothesize, study, develop, test and manufacture products is directly related to the quality and availability of information.

Our founders, Herb Boyer and Bob Swanson, were the first to conceptualize the process of cloning human proteins for the purpose of manufacturing life-saving therapies. Vital to this process then and now, nearly 20 years later, is the ability to access patient data—past, present and future. I will not testify today that new federal standards that limit our ability to access patient data will eliminate biomedical research as we know it. I will say, however, that without responsible access to such information, patients will be the true losers as patients will have access to fewer, more expensive therapies.

The medical research community depends upon uniform standards for the performance of clinical and medical investigations. As we consider new important legislation aimed at protecting the privacy and confidentiality of patients from abuse, we need to be certain that this legislation does not erect unnecessary barriers that slow and impede medical research. To do so will adversely impact all future generations who are dependent on the steady progress of medical research in order to improve their lives as they encounter and struggle with the consequences of illness and disease.

The United States is unquestionably the world's leader in medical research. With appropriate pride, we can point to our academic research institutions, the National Institutes of Health (NIH) and the Center for Communicable Diseases (CDC), to name a few of the more prominent institutions. The United States is home to lead-

ers in all types and varieties of medical research from epidemiology and outcomes research on one hand to the application of novel surgical techniques on the other. Our leadership, however, has been fostered by ready, uniform access to the key information and data contained in the patient's medical records. Our studies involve data as well as patients from all over the country, and the World, for that matter. We engage in partnerships with research entities, health plans and others also located across the 50 United States. I know that access to data drives research, particularly medical research, and access to patient's data has driven medical research in the United States since the turn of the 20th century when Flexner advocated a scientific basis for the training of physicians and the practice of medicine. Thus, uniform rules regarding how we may access and use this gold mine of information are critical to our underlying success. Let us consider some examples:

1. The Mayo Clinic was founded in 1907. The founders recognized the value of looking critically at their own experience, both in terms of the natural history of disease in their patients and the outcomes of their surgical and medical interventions. The Mayo Clinic has been a leader in the indexing of medical records, the application of the information technologies needed to search and retrieve information from their patient databases, and in outcomes research. Dr. Melton described some of the Mayo Clinic experience in an editorial in New England Journal of Medicine in 1997. He noted that more than 1,000 articles have been published in the medical literature based on the Mayo Clinic experience, and described particular difficulties associated with a law passed in Minnesota which has made it more difficult for the Mayo Clinic to conduct epidemiologic research by requiring specific patient authorization for the use of patient data.

Now that the Mayo Clinic has spread to at least three states (Florida, Arizona, and Minnesota), and is a pioneer in the development of a computerized medical record, we can look forward to even more productive information stemming from their experience, assuming that ill-advised legislation from states or the federal government relating to patient confidentiality does not dramatically erode our ability to use this information to further medical research.

2. The comparison of medical research done in the United States and Europe by pharmaceutical companies reveals some important insights. The United States is a preferred site for drug development. I believe this relates to the presence of uniform standards for pharmaceutical research supervised by the FDA as well as to the similar guidelines adopted by physicians and institutions in the United States. Compare our situation to the diverse array of regulatory agencies one encounters in Europe, not to mention the variations in language, culture, politics, and standards of medical practice. The implementation of different local standards of patient confidentiality in the United States will have the practical effect of erecting barriers to medical investigations of all kinds. Ultimately, these barriers will lead to inefficiency and a loss of the advantages now present in our country. Pharmaceutical companies care deeply about time, resource expenditures, and productivity. Should legislation lead to disincentives for pharmaceutical research, drug development efforts may well be shifted away from the United States towards more favorable environments.

3. Recently the National Registry for Myocardial Infarction (NRMI) showed that important differences exist between different regions of the United States in regard to the diagnosis and treatment of myocardial infarction or heart attacks. Women in general, and older women in particular, were much less likely to have their heart attack diagnosed and treated as compared to men. These differences varied significantly by region in the US. Uniform standards allow "outcomes research" to be done across our country and detect deviations that can be addressed. This type of research is critical for improving the quality and reducing the cost of treatment and care.

In the past few years significant progress has been achieved in the understanding of genomics in the metabolism of drugs and in drug interactions. The importance of drug metabolism was initially recognized as differences in pharmacokinetics and pharmacodynamics in racial sub-populations. Subsequently, the differences have been attributed to the genetic variations such as cytochrome P450 that are responsible for the metabolism of drugs. These differences are critical to understanding the safety and efficacy of many drugs across patient populations. The study of relevant sub-populations has become a common FDA requirement for the approval of many drugs. The majority of some of these sub-populations are concentrated in a few states. State regulations inhibiting access to patient records will have the unintended consequence of inhibiting access to information about the sub-populations of patients. As a result, we will know less about their diseases, the natural history of diseases in these subgroups, and the effects of medical and surgical treatment on their illnesses.

This is not just a theoretical argument. In the 1960's and 1970's, we routinely excluded women and children from research involving new drugs to "protect them." As a result, we had almost no information about the safety and activity of these drugs in women or children. Despite the absence of critical information, these same drugs were broadly used in the treatment of women and children once they were approved.

Another example is the FDA's regulations for filing an Investigational New Drug Application (NDA) prior to commencing studies in humans. This is a significant hurdle that is not present in the United Kingdom where research can be done on normal male volunteers with informed consent and approval from an Institutional Review Board (IRB). Many pharmaceutical companies, even those centered in the United States, are performing initial human studies in the United Kingdom. I maintain that unnecessary barriers create real disincentives for doing medical investigations and fewer investigations are not in the patient's best interests. Clearly, we need to avoid legislation that will produce similar unintended consequences in the future.

The economic rationale for a uniform standard for patient confidentiality is compelling. Diverse laws governing patient confidentiality will create a need for individual "tailored" programs aimed at gaining access to the data in patient's records. The variability and diversity between different states will create a level of unnecessary complexity. To address the complexity, researchers will need to spend more time and more money to accomplish their research goals. The consequences will be to increase the cost of research and reduce the number of investigations that are done. Smaller numbers of more expensive studies are not in the best interests of patients or our country.

To put this discussion in context, Genentech, Inc., as well as the HLC coalition, support the federal uniformity provisions included in legislation introduced yesterday by Senator Bennett (R-UT). Senator Bennett's bill, the "Medical Information Protection Act of 1999," provides for very thorough preemption of state law, creating a uniform, predictable environment for the research community while replacing current state law with a rational, comprehensive system of federal safeguards, responsibilities, limits and penalties. To date, this is the only legislative proposal that would effectively address concerns I described earlier, such as those of the Mayo Clinic, while not sacrificing any "protections" provided to patients.

Conversely, proposals introduced by Senators Jeffords (R-VT) and Dodd (D-CT) (S. 578), as well as Senators Kennedy (D-MA) and Leahy (D-VT) (S. 573), would undermine our ability to conduct broad, inclusive, population-based research using patient data by subjecting us to a new federal standard as well as several conflicting state law standards relating to use, safeguards and patient authorization. The Kennedy/Leahy bill is the most concerning. This proposal would establish a federal "floor," allowing any state law which is considered to provide "greater protection" than the federal law to remain in effect. Even disregarding the practical difficulty of determining such a subjective standard as what constitutes "greater protection," which would undoubtedly require litigation to mediate, this standard would clearly perpetuate the complexity and inconsistency that is state law which stifles the industry.

The Jeffords/Dodd approach is equally troublesome and curious. Rather than create a federal floor, this proposal would establish relatively strong federal preemption of state law, but only 18 months after enactment of the law, leaving any state law enacted prior to this time in full force and effect. This 18-month window provides an express invitation for disaffected states to enact new law which conflicts or is inconsistent with the new federal law, arguably placing research entities and patients at-risk.

Here is a practical example. In the wake of concern over genetics—the power of genetic information and its potential for abuse—some states require that "genetic" information be segregated from the rest of the patient's medical record and subject to different standards. Under the Kennedy/Leahy or Jeffords/Dodd proposals, any such state laws would likely remain in effect, either by virtue of already being in existence or by virtue of being considered more protective than the federal law. As a result, health plans, hospitals and providers would have to separate out "genetic" information from the rest of the patient's medical information and treat it differently.

This raises several practical concerns. First, the states may vary in terms of what is considered "genetic." Even assuming states could agree on what they define as "genetic," as a physician, I can assure you that virtually every piece of medical information is, by its very nature, genetic. Eye color, gender, the predisposition to breast cancer are all examples of genetic information. So, how do we, as a practical matter, separate this information out from other, "non-genetic" medical information. Second, state rules regarding segregation will vary. As such, we would be poten-

tially subject to 50 different sets of rules regarding segregation and use of this critical information. Finally, the practical implication of such limitations are devastating. The value of so-called genetic information is immeasurable and is directly responsible for the development of such breakthrough drugs as Herceptin, which provides, for the first time, real hope to women suffering from breast cancer and their families.

Rather, federal law should subject all patient health information, including genetic information, to the same strong standards for protection. While each of the Senate proposals would provide new federal standards for protecting all such information (albeit differently), the on-going ability of states to apply different law and the attendant lack of preemption of such state law, directly undermines this shared goal.

Thank you, Mr. Chairman, for allowing me to share with you Genentech's principles and concerns regarding patient confidentiality. This Committee has been a vital partner in assuring a stable and fruitful environment for biomedical research, as illustrated by your recent efforts on the Food and Drug Administration Modernization Act (FDAMA) and funding for the National Institutes of Health (NIH).

Please understand that the ultimate impact of this issue is no different, and is directly related to innovation and research. Be assured that we share your commitment to protecting and safeguarding patient information; after all, patients ultimately are our business. Also understand, though, that information is the lifeblood of research and to the ability of the health care delivery system to enhance and assure quality. Patients are deserving of one strong law that secures all such information equally, and provides one clear set of rules regarding how patient information must be safeguarded, how it may be used, and the penalties that will apply for any misuse.

We applaud this Committee's effort and look very forward to working with you and others toward the final enactment of strong, workable and, most importantly, uniform federal standards protecting the confidentiality of patient medical information.

The CHAIRMAN. Ms. Koyanagi.

Ms. KOYANAGI. Thank you, Mr. Chairman.

My name is Chris Koyanagi, and I am policy director with the Judge David L. Bazelon Center for Mental Health Law here in Washington, but I am testifying today on behalf of the Consumer Coalition for Health Privacy, which is a coalition of numerous groups representing the interests of those who will use the health system.

We think that privacy is in fact a first principle in terms of enhancing quality of health care, and without trust, patients are not going to use the health system or fully participate in their treatment.

I thought it was interesting how often this issue came up this morning, and you might be interested if I give you some of the statistics from a very recent survey on this question which is in my fully written statement.

I have seen a number of studies on this issue over the years, particularly with respect to mental health treatment, but this was a survey of individuals in California using all kinds of medical care. One in six people in that survey said they do not believe that their health care information is used appropriately; they believe it has been used, or misused in certain instances. And one in five of them said that they engage in some form of privacy protection, such as paying out-of-pocket; doctor-hopping, so they do not have a single consolidated medical record; they avoid giving information to their providers, or they give inaccurate information, or they ask the doctor not to write certain things down.

I think that this kind of behavior is something to expect if we move forward with legislation that does not provide consumer confidence in this area. Individuals, both consumers themselves and

the doctors, will respond if the legislation is not sufficiently protective, and in the end, this compromises health care quality, and it compromises the objectives of the health plans that are in fact seeking weaker privacy protections. In the end, the validity of their own information will not be as good.

We would like to see preemption, which is the issue that I was asked to specifically address this morning—we would like to see the legislation not preempt the existing State laws in this area. Federal legislation should provide a floor of uniformity but not a ceiling.

Currently, I think it is important to understand that all of the bills introduced and being seriously considered by this committee, including Senator Bennett's bill, are in fact stronger than nearly all the provisions in nearly all the State laws. The States have not moved aggressively forward in the general privacy protection area, partly because I think it has not been a major issue with the American public, although it is increasingly becoming so. So even the enactment of the weakest provisions that are before you will in fact create fore the health plans a very uniform set of rules for them to follow in terms of privacy protections.

There is also no precedent for overruling the State flexibility in this area when you look at civil rights law and Federal privacy law. The banking industry, the credit laws in communications and in all these areas which are very interstate in terms of their commerce, allow States to continue to build upon the Federal floor and add greater protections.

I think the experience of some of the States where we do see the more intense protections for consumers is also important. They are usually in specific areas—some of them were cited earlier this morning, including by Senator Leahy, the Cancer Registry in Vermont—where particular States have particular situations where they need certain protections for privacy that may not be thought about in terms of the Federal statute.

In addition, where States have moved forward perhaps too aggressively—and here, I think it is very important in terms of reassuring some of their health plans and researchers—they have reversed themselves. Maine enacted a highly protective privacy law which was in force a very, very short period of time before it was put on hold because of the implications and the unforeseen consequences of that legislation.

And Minnesota, which enacted legislation with respect to research—which is very rare, incidentally, among the States—also amended its legislation when it became apparent that that was in fact a barrier to legitimate research.

So I think the States are quite capable of legislating in this area. They will move forward on specific issues that are important to their constituencies in their particular part of the country. And they will not behave irresponsibly, and if they make mistakes, they will reverse themselves. And States, I think, can reverse themselves more quickly than could the Federal Government. So I think it is important for you to continue to allow the flexibility at the State level that is in the Leahy-Kennedy bill and partly in your legislation, although in your legislation, that would end after a set period of time.

And I think also in this area, it is important to understand why people request preemption of State laws. If this legislation is about protecting individual privacy, which I believe your bill and Senator Leahy's bill truly are, and that is the perspective and where the bills begin, then there is no reason to restrict States from going further than your Federal legislation.

On the other hand, if this bill is about making the management problems of multiState health plans easier, then you would begin from the other end, and you would say that you want a single uniform standard around the country.

So I think this issue actually goes to the heart of why you are passing legislation, and if you wish to protect patient privacy, I would urge you to permit the States to go beyond whatever may come from the Congress in this first stab at a very difficult area and see watt happens. If there are in fact significant problems with State actions following enactment of the Federal law, you can come back and revisit it, but in the meantime, with technology roaring along, as some of the members of the committee have pointed out, I think it is very, very important to let the States have that flexibility in the future.

Thank you, Mr. Chairman.

[The prepared statement of Ms. Koyanagi follows:]

PREPARED STATEMENT OF CHRIS KOYANAGI

I. INTRODUCTION AND OVERVIEW

Mr. Chairman and Members of the Committee: I very much appreciate the opportunity to testify before you today on the preemption of state laws relating to medical privacy, confidentiality, and security. I am Chris Koyanagi, Policy Director for the Judge David L. Bazelon Center for Mental Health Law in Washington D.C. The Bazelon Center is a legal advocacy organization concerned with the rights of persons with mental impairments.

I testify today on behalf of the Consumer Coalition for Health Privacy (CCHP), a broad coalition of consumer, disability and patient advocates. The mission of the Consumer Coalition for Health Privacy is to educate and empower healthcare consumers to have a prominent and informed voice on health privacy issues at the federal, state, and local levels. Members of the coalition are committed to the development and enactment of public policies and private standards that guarantee the confidentiality of personal health information and promote both access to high quality care and the continued viability of medical research. The Coalition is an initiative of the Health Privacy Project, Georgetown University Medical Center.

As a member of the Coalition's Steering Committee, I have been working with my colleagues in the disability rights, consumer, and patient advocacy communities to make the case that protecting privacy must be a "first principle" of enhancing the quality of health care, of fostering research and public health initiatives, and of broadening access to critical health care services. We believe that without trust that the personal sensitive information that they share with their doctors will be handled with some degree of confidentiality, patients will not fully participate in their own health care.

A survey released by the California HealthCare Foundation in January 1999 found that "public distrust of private and government health insurers to keep personal information confidential is pervasive. No more than about a third of U.S. adults say they trust health plans (35%) and government programs like Medicare (33%) to maintain confidentiality all or most of the time."[1] The consequences of such distrust—real or perceived—are significant. The Foundation's survey identified that:

- One in every six people believe their health information has been used or disclosed inappropriately.
- One of five people engage in some form of "privacy-protective" behavior when they seek, receive or pay for health care in this country. Such behavior includes pay-

[1] The poll was conducted for the Foundation by Princeton Survey Research Associates. The survey topline is available at http://www.chcf org.

ing out-of-pocket for care; intentionally seeing multiple providers to avoid the creation of a consolidated record; giving inaccurate or incomplete information on a medical history; asking a doctor to not write down the health problem or record a less serious or embarrassing condition; and even not seeking care to avoid disclosure to an employer.

The consequences of people not fully participating in their own care are quite troubling, for individual patients as well as the larger community. For instance, incomplete or inaccurate' information can hamper a doctor's ability to accurately diagnose and treat a patient, inadvertently placing a person at risk for undetected and untreated conditions. In turn, if doctors are receiving incomplete, inaccurate information, the data they disclose for payment, research, public health reporting, and outcome analysis will be unreliable. Ultimately, information that lacks integrity at the front end will lack integrity as it moves through the health care system. Thus, protecting patient privacy is integral both to improving individual care, and to the success of public health initiatives and quality of care.

Members of the Consumer Coalition are keenly aware of the importance of good, solid data for research. As health care patients and providers, our members stand to benefit the most from advances in research, public health initiatives, and improvements in quality of care. People with disabilities, in particular, are frequent users of health care services, and are also deeply invested in ensuring that the health care system operates efficiently and effectively. As such, the Consumer Coalition for Health Privacy is committed to ensuring that protecting privacy and promoting health are values that must go hand-in-hand.

Toward this end, the Consumer Coalition has established a set of health privacy principles to guide our efforts (see attached principles and sip-on). We believe that public policy in this area should guarantee individuals: a right to see their own medical records; the ability to exercise voluntary, informed choices about the use of their health information; a court order or warrant requirement for law enforcement access to medical records; and a comprehensive set of enforcement mechanisms.

We hope that Congress will meet the deadline established in the Health Insurance Portability and Accountability Act (HIPAA) to pass comprehensive health privacy legislation by August 1999, and we also hope that the new law will go a long way in helping us to meet these public policy goals set forth in our principles. However, in many ways, one of the most critical issues for the Coalition is preemption. **The Coalition arrived at a firm consensus that "federal legislation should provide a floor for the protection of individual privacy rights, not a ceiling."**

All three of the health privacy bills pending in the Senate preempt weaker state laws. At issue here is how a federal health privacy law will relate to existing and future stronger state laws. Will Congress choose to establish a federal "floor" above which states would be free to enact greater protections? Or will the federal law fully preempt state laws by creating a "ceiling," thus eliminating both weaker and stronger state laws and preventing the passage of future stronger state laws?

All three health privacy bills take a different approach to preemption:

- S. 573, Medical Information Privacy and Security Act (MIPSA), introduced by Senator Patrick Leahy (D-VT) and Senator Edward Kennedy (D-MA), proposes establishing a federal floor that would eliminate all weaker state laws, while allowing heightened state protections to stand. [2]
- S. 578, Health Care Personal Information Nondisclosure Act of 1999 (Health Care PIN Act), introduced by Senator James Jeffords (R-VT) and Senator Christopher Dodd (D-CT), proposes to grandfather in existing state laws with heightened protections, and establishes an 18 month window in which states can pass stronger laws until total preemption is the prospective rule.
- A draft bill circulated by Senator Robert Bennett (R-UT), Medical Information Protection Act of 1999, proposes to fully preempt state laws that extend heightened protections. State laws providing greater protection than the federal law would be eliminated, and states would be prohibited from passing medical privacy laws in the future.

Only the approach embodied by S. 573, the Leahy/Kennedy bill, mirrors the Coalition's principle on preemption. Again, we strongly oppose federal preemption of state laws that provide greater consumer protections—including heightened safeguards for certain medical conditions and circumstances. Our testimony today is intended to demonstrate that the federal law should establish a floor of protections, not a ceiling. We believe that a fully-preemptive federal law in this area is unprecedented, unwise, and may be a danger to public health.

---

[2] A companion bill, H.R. 1057, was introduced in the House of Representatives by Representative Edward Markey (D-MA)

Our testimony highlights specific state laws at risk of being preempted under a total preemption approach, as reflected in the Bennett draft. It should be emphasized, however, that preemption is a moving target. Until there is a consensus bill, it will be impossible to determine the full impact of preemption.

The Consumer Coalition for Health Privacy opposes the preemption of stronger state laws for the reasons outlined in this testimony.

II. THE NEED FOR UNIFORMITY

Congress will create a high level of uniformity simply by preempting weaker state laws. Passage of any of the proposed Senate bills will result in substantially greater uniformity, given that all three bills preempt weaker state laws. Simply by preempting these weaker state laws, Congress will eliminate the vast majority of state laws and create a high degree of uniformity.

Preliminary research on state health privacy laws conducted by the Health Privacy Project shows that most state laws governing the broad areas sought to be regulated by the federal bills—patient access to records, notice of information practices, patient authorization for disclosure, remedies for violation of the law—would fall under the floor laid down by the Senate bills.

Consider the state of affairs today: health care entities that do a great deal of business across state lines are currently required to comply with fifty different—and often conflicting—state laws. At the same time, the vast majority of these laws are weaker than the standards proposed in all three Senate bills. Therefore, far from adding additional burdens, the federal law will provide a substantial degree of uniformity simply by preempting weaker state laws. A federal floor—if it is set at an appropriate level—will actually standardize the vast majority of health privacy and security practices.

Moreover, there is no evidence that the interplay between state and federal laws in these areas significantly interferes with interstate commerce. The Right to Financial Privacy Act, the Fair Credit Reporting Act, and the Electronic Communications Privacy Act regulate the banking, credit, and communications industries, all of which conduct extensive business across state lines. All of these laws, however, leave states free to enact more protective laws as they see fit.

III. PRECEDENT IN FEDERAL CIVIL RIGHTS AND PRIVACY LAW

No precedent exists in federal privacy or civil rights law for preempting stronger state laws. In the past, when Congress has considered preemption, it has recognized the importance of allowing states to address issues unique to the states and their citizens. Historically, the federal government establishes a "floor" of protections, leaving the states free to provide greater protections.

The proponents of total preemption express fear that states will pass laws that are "too privacy protective," thereby interfering with important health-related activities. But the facts are reassuring: states have been quick to respond to the concerns of health care plans, researchers and others. **Where a "privacy protection" was deemed to interfere with vital health care functions, states have quickly amended their laws.** Minnesota, for example, amended a law relating to researcher access to medical records after hearing objections from health care organizations in the state. More recently, Maine postponed implementation of a health privacy law after objections on the part of press and family members.

Many states are considering pending health privacy bills, in an attempt to fill the vacuum created by the existing gap in federal health privacy law. However, in the past, following the passage of comprehensive federal legislation, the momentum behind such state initiatives drops significantly. After passage, state activity is likely to reflect the standards proposed in the federal law, thereby increasing uniformity.

IV. STATE LAWS MORE DETAILED AND NUANCED

State health privacy laws address a level of detail not found in any of the federal proposals. For the most part, state health privacy laws are organized by entity, and the statutes include requirements and specifications explicitly related to that entity. There may be separate statutes governing many different entities: employers, nursing homes, Health Maintenance Organizations, health and life insurers, psychiatrists, chiropractors, hospitals and insurers.

In addition, there are numerous issues traditionally acted on at the state level that include privacy provisions. These include anti-discrimination laws, commitment proceedings for the mentally ill, adoption, foster care, mental health treatment, reproductive health, parental involvement, partner notification, and abuse and neglect.

In comparison, the federal proposals have, on the whole, treated all health care organizations in a similar fashion. The federal proposals have also established—with a broad brush—general rules about the use or disclosure of health information. These rules will address the vast majority of circumstances in which health informa-

tion is used and disclosed, but they do not approach the level of detail that has been developed at the state level over many years.

• California law provides patients a right to see and copy their own medical record, as do all the Senate proposals. The state law, however, also explicitly provides that access can not be denied because the individual owes money for past services. [3]

• Maryland has an intricate statutory system for dealing with mental health records. The disclosure of mental health records is governed by the state's Confidentiality of Medical Records Act. One provision stipulates that mental health records may not be disclosed between health care providers that participate in an approved plan of a core service agency [4] for the delivery of mental health services unless a patient has received a current list of the participating providers and has signed a written agreement to participate in the client information system developed by the agency. [5]

5Maryland Id. At Sec. 4-307 (e).

• Vermont requires the Health Commissioner to maintain a cancer registry and to keep all information confidential, except in limited circumstances. [6] Most of the Senate bills would allow for greater disclosure of the information maintained in the registry than is currently permitted under Vermont law. Many states have established similar cancer registries by statute.

Such a level of detail is not even contemplated by any of the federal proposals, and regulating these spheres is clearly not the intent of any of the federal proposals. By fully preempting state law, Congress would likely preempt important state laws without providing an equal level of guidance, or necessary protections.

V. VALUE OF "HEIGHTENED PROTECTIONS" AT THE STATE LEVEL

All of the proposed Senate bills treat all health information the same. Unlike the state laws, the proposals do not establish specific rules for certain kinds of information.

The result is that even the strongest federal proposals have not set the bar as high as some state laws. If any of the current federal health privacy proposals were to pass with a preemptive federal ceiling included, the citizens of some states would actually forfeit the protections they are now guaranteed under their state laws.

• California has enacted a number of HIV/AIDS specific confidentiality laws, covering testing, reporting, partner notification, and discovery. The results of an HIV/AIDS test may not be disclosed in a form that identifies an individual, without patient consent for each disclosure, except in very limited circumstances. For instance, a physician or local health officer may disclose HIV test results to the sex or needle-sharing partner of the patient without consent, but only after the patient refused or was unable to make the notification. The law also requires patient authorization in more circumstances than provided for under the Senate proposals. In California, an individual's health care provider may not disclose to another provider or health plan without written authorization, unless to a provider for the direct purposes of diagnosis, care, or treatment of the individual. [7]

• In Georgia, heightened protection is given to information derived from genetic testing. This information is considered to be strictly confidential and may be released only to the individual tested and to persons specifically authorized by such individual to receive the information. Any insurer that possesses information derived from genetic testing may not release the information to any third party without the explicit written consent of the individual tested. [8]

• New York has a comprehensive set of statutes providing additional protection of the confidentiality of HIV related information. New York generally prohibits the disclosure of HIV related information without the patient's consent. Accordingly, a patient's consent to the release of HIV related information specifically limits to whom disclosure may be made, the purpose for such disclosure and the time period during which the release is effective. Unlike the federal proposals, a general authorization for the release of medical information does not encompass the disclosure ofH1V related information unless it specifically states so. [9] In enacting these stat-

---

[3] California Health and Safety Code, Section 123 100 et seq.

[4] A "core service agency" is an organization approved by the Mental Hygiene Administration to manage mental health resources and services in a designated area or to a designated target population. Md. Health -General Code Ann. Sec. 4-307(a)(3) (1999).

[5]

[6] 18 V.S.A. Sections 154 et seq.

[7] See California Health and Safety Code, Section 120975 et seq; 121015 et seq, Insurance Code, Section 799 et seq.

[8] Ga. St. 33-54-3.

[9] NYCLS Public Health Law Sec. 2780 et seq.

utes, the New York legislature expressly stated that it intended to "encourage the expansion of voluntary confidential testing for . . . HIV so that individuals may come forward, learn their health status, make decisions regarding the appropriate treatment, and change the behavior that puts them and others at risk of infection." [10]

• Tennessee law stipulates that the State Department of Health records on STI)s may not be released even under subpoena, court order, etc. unless the court makes a specific finding concerning each of five criteria including: weighing probative value of the evidence against the individual's and public's interest in maintaining its confidentiality; and determining that the evidence is necessary to avoid substantial injustice to the party seeking it and either that the disclosure will not significantly harm the person whose records are at issue or that it would be substantially unfair as between the requesting party and the patient not to require disclosure. [11] *This standard is higher than the standard established in both the Jeffords/Dodd and the Bennett/Mack bills.*

Many states have laws similar to the ones cited above for certain information such as mental health, genetic tests, and HIV/AIDS. Again, none of the federal proposals reach these levels of protection. In some circumstances, states enacted these heightened protections to respond to critical public health issues. Wiping out such laws could create a public health crisis, leaving people vulnerable by undoing protections that encourage people to seek testing, counseling, and treatment for a number of conditions.

VI. THE DANGER OF UNINTENDED CONSEQUENCES

Laws relating to the confidentiality of medical information are found throughout state codes. In California, for example, citizens have a right to privacy in the State Constitution. Major statutes are found in the Civil Code, the Insurance Code, the Health and Safety Code, the Penal Code, and the Welfare and Institutions Code. The laws cover a wide range of activities including treatment, payment, insurance-related activities, peer review, research, and prescribing drugs. Most importantly, states have developed bodies of law around-discreet issues—that touch on the use of health information—such as anti-discrimination, worker's compensation, parental involvement, adoption, HIV/AIDS partner notification, and access by law enforcement, and even real estate.

It is not possible to predict in advance the full impact of such broad preemption on state law and consumer protections. The "relating to" language used to preempt state law in some federal proposals casts a wide net in terms of the state laws that would be eliminated completely. **The preemption of all state law "related to" the federal law could have significant unintended consequences.**

• At risk of being preempted is a California law that prohibits insurers from discriminating on the basis of a person's "genetic characteristics that may, under some circumstances be associated with disability in that person or that person's offspring." The law includes a provision on authorization requirements for the disclosure of genetic information, which may open up the entire statute to preemption. [12]

A larger issue is at hand. Many state health privacy laws were enacted specifically to address public health concerns. Mental health and HIV/AIDS confidentiality laws, for example, were enacted specifically to encourage people to seek appropriate care, without fearing harmful reprisals.

The states are best equipped to respond to many new, unique, and inherently local challenges in health care and public health. It is impossible to predict what issues will require prompt attention in the future, but a preemptive federal law would prevent states from responding at all.

VII. CONCLUSION/

Most importantly, Congress will create a high level of uniformity simply by preempting weaker state law with a strong federal law. This is true under any of the three Senate health privacy proposals—the research of state health privacy laws bears this out. Thus, there is no overriding justification to totally preempt state law in order to achieve substantial uniformity.

The interests of health care consumers and providers will be best served by Congress establishing a federal floor that leaves the states free to enact greater protections, as Congress has done for every other privacy and civil rights laws, regardless of how complex or interstate the area to be regulated. Such a solution would allow the states to address the specific—and unique—needs of their citizens while providing a great deal of national uniformity regarding the use and disclosure of health information. A federal ceiling, on the other hand, could have profound negative con-

---

[10] NY Laws 1988, ch 584, Sec. 1.
[11] Tenn. C.A. Sec. 68-10-113 6(A).
[12] Insurance Code, Section 10140 et seq.

sequences for consumers and health care providers by inadvertently eliminating important protections, or restricting the ability of states to respond to the privacy needs of their residents.

Passage of a federal health privacy law will necessarily involve compromises. The stakeholders are diverse, as are the states and their constituencies. It is appropriate that the federal law would reflect these compromises, but it raises a troubling possibility: that the federal law will set a relatively low standard and preempt state law. This is the worst-case scenario. The result would be to eliminate existing state protections without replacing them with comparable federal standards, locking the states out of taking steps to address local health needs.

We urge this Committee, and the rest of the Congress, to resist the proponents of total preemption. Such a radical approach would undo legal protections put in place by states responding to pressing public health concerns.

In order to encourage people to seek testing, counseling, treatment, and other health care services, many states have established heightened protections for people with mental illness, HIVAEDS, drug and alcohol dependence, and other circumstances where people face stigma, discrimination, and embarrassment. If these safeguards were wiped off the books, as they would be under the Bennett draft bill, the most vulnerable people in our communities would immediately be put at risk of exposure, and faced with the cruel choice of either protecting their privacy or seeking health care. Such a result, we believe, would substantially undermine state—and national—health initiatives.

Rather than undermining our nation's existing system of checks and balances, we should continue the tried and true practice of allowing states to decide when it is appropriate to provide consumer protections stronger than the federal law.

Statement of Mission and Principles

(3/22/99)

The mission of the Consumer Coalition for Health Privacy is to educate and empower health care consumers to have a prominent and informed voice on health privacy issues at the federal, state, and local levels. Members of the coalition are committed to the development and enactment of public policies and private standards that guarantee the confidentiality of personal health information and promote both access to high quality care and the continued viability of medical research. In order to accomplish these goals, health privacy policy must be based on the following principles:

—Right to Privacy

An individual's right to privacy with respect to individually identifiable health information, including genetic information, should be established statutorily. Individuals should retain the ultimate right to decide to whom, and under what circumstances, their individually identifiable health information will be disclosed. Confidentiality protections should extend not only to medical records, but also to all other individually identifiable health information, including genetic information, clinical research records, and mental health therapy notes. Additional protections may be necessary for highly sensitive information.

—Identifiable Information

Use and disclosure of individually identifiable health information should be limited. Protections should be in place to ensure that anonymized data is used whenever possible.

—Access

An individual should have the right to access his or her own health information and the right to supplement such information. Individuals should have the right to access and supplement their own medical records so that they can make informed health care decisions and can correct erroneous information in their records.

—Notice

Individuals should be notified about how their medical records are used and when their individually identifiable health information is disclosed to third parties. Individuals should be given written, easy-to-understand notice of how their individually identifiable health information will be used and by whom. With such notice people can make informed, meaningful choices about uses and disclosures of their health information.

—Informed Consent

The use or disclosure of individually identifiable health information absent an individual's informed consent should be prohibited. Health care providers, health plans, insurance companies, employers and others in possession of individually identifiable health information should be prohibited from using or disclosing such information unless the use or disclosure is authorized by the individual. Use or disclosures without informed consent should be permitted only under exceptional circumstances—for example, if a person's life is endangered, if there is a threat to the

public health, or if there is a compelling law enforcement need. Disclosure of individually identifiable health information for marketing or commercial purposes should never be permitted without informed consent. Any time information is used or disclosed it should be limited to the minimum amount necessary for the use or disclosure.

—Public Health and Research

While protecting individual privacy rights, legislation should not impede important public health efforts or clinical, medical and quality of care research.

—Safeguards

The development of security safeguards for the use, disclosure and storage of personal health information should be required. Appropriate safeguards should be in place to protect individually identifiable health information from unauthorized use or disclosure.

—Penalties

Strong and enforceable remedies for violations of privacy protections should be established. Remedies should include a private right of action, as well as civil penalties and criminal sanctions where appropriate. Individuals that come forward to report violations of this law should be protected from retaliation.

—Preemption

Federal legislation should provide a floor for the protection of individual privacy rights, not a ceiling. Like all other federal civil rights and privacy laws, federal privacy legislation for health information should set the minimum acceptable standard. Federal legislation should not pre-empt any other federal or state law or regulation that is more protective of an individual's right to privacy of or access to individually identifiable health information.

Endorsing Organizations (In formation)

AIDS Action, AIDS Policy Center for Children, Youth, and Families, American Association of Occupational Health Nurses, American Counseling Association, American Federation of State, County, and Municipal Employees, American Nurses Association, American Pseudo-obstruction and Hirschsprung's Disease Society, American Psychiatric Nurses Association, Americans for Democratic Action, Association of Women's Health, Obstetric and Neonatal Nurses, Bazelon Center for Mental Health Law, Call for Action, Center for Reproductive Law & Policy, Center for Women Policy Studies, Children and Adults with Attention Deficit/Hyperactivity Disorder, Committee for Children, Consumer Federation of America, Easter Seals, International Union, UAW, Legal Action Center, Les Turner ALS Foundation, Myositis Association of America, National Abortion Federation, National Association Mandating Equitable Databases (the NAMED), National Association of Alcoholism and Drug Abuse Counselors, National Association of People with AIDS, National Association of Social Workers, National Black Women's Health Project, National Family Planning and Reproductive Health Association, National Gay and Lesbian Task Force, National Health Law Program, National Latina/o Lesbian, Gay, Bisexual and Transgender Organization, National Multiple Sclerosis Society, National Organization for Rare Disorders, National Organization for Women, National Partnership for Women & Families, National Senior Citizens Law Center, Planned Parenthhood Federation of America, Service Employees International Union, and Title II Community AIDS National Network.

The CHAIRMAN. Thank you.

Dr. Curd, the issue of preemption of State laws is one of the most difficult ones. If it is safe to assume that Genentech currently uses medical information from all over the United States in its research, how does Genentech currently deal with the differing State laws?

Dr. CURD. We do the best we can. And in fact, to be really quite honest with you, when somebody brings me a list of 50 potential sites for a clinical investigation, one of the things that goes into the equation about whether or not we use them is their past performance, the difficulties of getting things through their IRB, and their ability to enroll.

So what I would tell you, for instance, is that the University of California education system is really a pain. They are really difficult, whereas I can do things at the Mayo Clinic or in Utah or in New Mexico or in Texas much more easily. That is time and money, and it ultimately turns into quality science. If I can enroll

100 patients in a study in 3 months versus maybe 100 patients in 2 years, that makes an enormous difference to the pace and the quality of research.

So we are influenced by one of the factors being how restrictive or how nonrestrictive is it to do research there.

The CHAIRMAN. You mentioned the Mayo Clinic in Minnesota. Could you speak to California State law and what implications it has for your research?

Dr. CURD. Right now, there is a whole proliferation—I am actually not qualified to say—I think there are probably six or seven different, conflicting bills ongoing now in the State legislature in California, some of which will be a nightmare for companies like Genentech. So at least Minnesota at this point has one law, and we know what it is.

What is interesting from my point of view is that if I want to work with the Mayo Clinic, and I am actually dealing with Florida, Arizona and Minnesota, does the Minnesota law apply to the Mayo Clinic patients who are in Florida, or not?

So again, it makes it more complex, and I think the data that I tried to cite about what is going on with the Mayo Clinic, with a 100-year good record in terms of patient-related research, says that their system is being eroded and may be devastated by the fact that patients just do not understand watt they are consenting to.

In fact, I wanted to quote from an article that came out in April. They went back to the patients who did not send in their cards and did not consent and talked to them in focus groups. They say: "Most participants in the focus groups were unaware that this type of research is the source of most prognostic and outcomes data that could be used for making crucial health care decisions for themselves." Most patients when they are asked to sign one of these consents are thinking about that important issue of personal private medical information, and not about the altruistic things for society.

So again, I think we have a real dilemma here that requires uniform standards across the United States by a body like yourselves.

The CHAIRMAN. My bill as well as Senator Bennett's bill allow State laws to continue with respect to public health activities. Knowing that you support strong Federal preemption, do you support a limited carve-out for public health law?

Dr. CURD. We have a long history of certain public health issues that really are dealt with on the State level—reportable diseases, infectious diseases like AIDS and so on—so I would say yes.

The CHAIRMAN. Ms. Koyanagi, in your testimony, you comment that a Federal standard that creates a floor will in essence preempt many of the laws that currently exist, because they are weaker. Do you believe it is possible for Congress to pass one uniform standard which is strict enough so that the States will not continue to pass tougher laws?

Ms. KOYANAGI. Well, obviously, where you place the bar will have a lot to do with whether States would continue to legislate in this area. But I think one thing that is very important to recall is the comment earlier this morning that we do not really know today some of the issues that we might be facing even 2 years from now

in terms of privacy with the increased explosion of information systems and use of the internet. A few years ago, we would not have thought about genetics information needing to be protected.

So I think that while it is conceivable that you could pass a Federal bill that is so progressive, in my view, that it would negate that chance that States would add, or even wish to add if they had the flexibility, further protections, I think none of us can be quite sure what might be just around the corner. And I do think that States are probably in a better position to act quickly than is the Federal Government in that area.

The CHAIRMAN. Should we consider a legislative proposal that preempts State law except in the areas of mental health, public health reporting, and a few other narrow exceptions?

Ms. KOYANAGI. Well, of course, as an advocate for people with mental illness, I am very, very aware of the particular sensitivity of that information and of some other areas of health care. But I think it is reasonable to ask why, if these protections are so important for sensitive information, they would not be equally useful for all medical information.

I think that we really do not fully understand how concerned people can be about the release of what may seem to us to be fairly routine information; this can vary from person to person. And if it is possible to put in procedures that are fully protective of sensitive information, it should be fairly simple to use those procedures for other information. So we would not at this stage suggest picking and choosing in terms of State preemption.

The CHAIRMAN. In your testimony, you discuss the problems with Minnesota and Maine laws where State legislators went back in to fix some of the provisions. Some would argue that Congress can learn from these mistakes and create a workable Federal standard. Would you agree?

Ms. KOYANAGI. I would hope so, yes.

The CHAIRMAN. You would hope, anyway.

Ms. KOYANAGI. And we would love to help you.

The CHAIRMAN. As we have heard today, many State laws are organized by entity, such as hospitals or health plans, and may have separate statutes governing them. As our system becomes increasingly integrated, would consistency in standards, whereby all entities have the same responsibilities and penalties for violation of the law benefit the patients?

Ms. KOYANAGI. Yes. We very strongly support enactment of this legislation. I think it would do much to protect privacy and to create appropriate standards across all health care settings, so we very strongly support that.

Our concern about the State flexibility is only that this is a new area of law, and it is very, very complex. We do not have confidence that we will see the bar on privacy sufficiently high by the time legislation comes out of the Congress, and if that is so, we just continue to think it is important for States to have additional rights to protect privacy.

But yes, I think this legislation is very, very important, and we strongly support your moving forward on these bills as soon as possible.

The CHAIRMAN. Dr. Curd, do you have any final comment?

Dr. CURD. I think the key thing here is that the United States is the world's leader in medical research. The quality of the technology in our medical system probably beats everybody else. That did not happen by chance. It has really happened through a very coordinated effort that has involved medical research, the NIH, the CDC, industry, and the cooperation of the whole United States. And that is a very valuable asset, and I would certainly hate to see us lose a position of leadership because we had some unintended consequences of trying to do another very important thing on an individual basis, which is protect patient confidentiality.

Every one of us is or will be a patient, and we want our private rights protected, and if somebody abuses mine, I want them punished. But on the other hand, I do not want my children in 10 or 15 years to not have access to important new treatments because we could not get population data that told us what needed to be done.

The CHAIRMAN. Thank you. I am very sensitive to your comments, and we will be watching that very closely. Of course, we also have NIH and a few other organizations under our review, so——

Dr. CURD. Well, we are counting on you.

The CHAIRMAN. All right. Thank you very much.

I want to thank all of the witnesses.

Members will have an additional 2 weeks to submit questions to the witnesses, and at this point, I am ready for lunch.

[Additional statements and material submitted for the record follow:]

PREPARED STATEMENT OF SENATOR HAGEL

Good morning, Mr. Chairman. Thank you for calling this timely and important hearing.

The issue of medical record confidentiality is not a simple one. Many patients believe that their individual information is confidential and will never be used for anything other than medical care. However, that is not necessarily true. There are many disclosures of a patient's individual information. Some of this disclosure the patient has consented to while other disclosures are made without consent.

The question that we must answer is how do we balance keeping an individual's personal information protected while not stifling health care, medical research, the actions of law enforcement, and many other important activities.

The passage of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) placed a deadline of August 1999, for Congress to implement privacy legislation. If not, HIPAA requires the Secretary of Health and Human Services to implement comprehensive privacy regulations. The August deadline is soon approaching. It is imperative that Congress acts quickly.

Today, we have a patchwork of state laws that govern medical record confidentiality. Unfortunately, in many states this legislation is found in different areas of State law—public health, banking, insurance, etc. There is no uniformity or reliability to these laws. This is making it very difficult to judge exactly what the current status of medical record privacy is in the United States.

As Congress approaches the task of creating comprehensive privacy legislation, some of the most important areas that must be addressed include authorization from the patients, law enforcement rights, medical research and the possibility of preempting current state laws. As I stated earlier, this is not a simple task. Once one issue is resolved, it seems as though another 50 issues arise. Congress has a difficult road ahead, but a very important one that needs to be addressed with thoroughness, foresight and creativity.

I look forward to hearing from the panelists today on their thoughts about medical record confidentiality.

Thank you, Mr. Chairman.

STATEMENT OF THE AMERICAN PSYCHOANALYTIC ASSOCIATION

Mr. Chairman and members of the Committee, my name is Robert Pyles and I am President of the American Psychoanalytic Association. We appreciate the opportunity to present our concerns on the issue of "Medical Records Confidentiality in a Changing Health Care Environment."

Our principal concern is that privacy legislation protect and preserve the "atmosphere of confidence and trust" which permits psychotherapy patients "to make a frank and complete disclosure of facts, emotions memories and fears" that is essential for effective psychotherapy. See Jaffee v. Redmond, 116 S.Ct. 1923, 1928(1996).

We have been shocked by how little consideration has been given to the historical and traditional treatment of this issue. Such consideration is a fundamental first step in any legal analysis and was the approach taken by the Supreme Court in the 1996 decision in Jaffee v. Redmond. As the Court correctly noted, "reason and experience" (essentially the historical treatment of privacy in the psychotherapy context) show that "the mere possibility of disclosure may impede development of the confidential relationship necessary for successful treatment". That conclusion was based on a review of standards of medical ethics from Hypocrites to the present, numerous reports of empirical research, the deliberations of the 1972 Judicial Conference Advisory Committee and the statutory laws in all 50 states.

The findings and rationale of Jaffee v. Redmond, led the Court to recognize that communications between a psychotherapist and a patient are "privileged" and therefore, not subject to discovery and disclosure in judicial proceedings. Those findings and rationale lead to the obvious conclusion that comparable protection must be afforded privileged psychotherapy communications even outside of the judicial context. Otherwise, health plans and others would be permitted routine access to health information that they would be barred from obtaining in a court of law. The effectiveness of psychotherapy services also would be routinely be destroyed.

This was precisely the conclusion of the Health Care Financing Administration of the Department of Health and Human Services in an opinion issued on March 11, 1999. In that opinion, HCFA noted that the privileged nature of psychotherapy communications is "firmly rooted" in the federal common law as well as the common law of all 50 states. Therefore, HCFA concluded that the federal government could not gain access to mental health communications that might fall within the privilege unless the patient waives the privilege.

Accordingly, there is already a federal law which provides a "floor" of protection for the privacy of psychotherapy communications. Communications between a therapist and a patient during the course of psychotherapy are "privileged" communications and are not subject to disclosure beyond the therapist without the patient's consent. This "privilege" is no less strong than the widely acknowledged "attorney-client" privilege and exists for similar reasons. The attorney-client privilege is recognized to "encourage the full and frank communication" between attorneys and their clients and thereby "promote broader public interests in the observance of law and the administration of justice". The psychotherapist-patient privilege serves the public interest by "facilitating the provision of appropriate treatment for individuals suffering from the effects of a mental or emotional problem". Jaffee v. Redmond, 116 S.Ct. at 1929.

Even where the government pays for the cost of legal services such as under the Legal Aide Services program, the Equal Access to Justice Act or the Social Security Act, that financial interest does not give the government the right to gain access to the communications between the attorney and his or her client. Neither does that financial interest give the government the right to compel the patient to consent to the disclosure of those communications as a condition of the payment of appropriate

legal fees. Even where a private litigant pays the legal fees of his or her opponent as part of a settlement or court decision, that financial interest does not confer a right to gain access to the communications which gave rise to the costs of the legal services.

Similarly, the economic interest that a health plan has in the delivery of health care services should not confer a right on the plan to compel disclosure of psychotherapy communications that fall within the therapist-patient privilege. As the Supreme Court concluded, protection of that information from disclosure is essential for effective services, and access to effective mental health services is in the best interest of both the individual and the public generally. Jaffee v. Redmond, 116 S.Ct. at 1929.

Therefore, one fundamental test that any medical information privacy bill must pass is, "Does the privacy legislation preserve the confidential relationship between the patient and the psychotherapist that is essential for effective services?"

The problems we find with The Health Care Personal Information Nondisclosure Act of 1999 (S. 578) are that, while the "findings" are consistent with the "reason and experience" identified by the Supreme Court, the protections in the bill are not consistent with the those findings. We offer the following examples and solutions:

1. Access to effective psychotherapy is eliminated for the less affluent.——

Section 2(1) and (2) correctly recognize that there is a "traditional right of confidentiality" between a health care provider and a patient that is now at risk.

Further, the findings correctly recognize that "[a]n erosion of the right of confidentiality may reduce the willingness of patients to confide in physicians and other practitioners, thus jeopardizing quality health care." Based on the analysis of reason and experience in Jaffee v. Redmond, we know that erosion of the right of confidentiality will eliminate effective psychotherapy.

The bill also correctly finds that an individual's confidentiality right means that his or her consent is needed to disclose protected health information, "except in rare and limited circumstances required by the public interest."

Problem—The problem arises in subsections 202(a)(2) and (3) which require health plans to obtain "blanket" consents for disclosure from patients for any information "in connection with treatment, payment, and health care operations". The effect of those provisions is to eliminate the right of confidentiality recognized in Section 2(1) of the bill for individuals who cannot afford to go without health insurance. Further, compelling such individuals to give their consent in order to obtain health insurance that they cannot afford to decline renders the consent meaningless for those individuals.

Also, subsections 202(a)(2) and (3) eliminate the very privilege recognized in Jaffee as essential for effective psychotherapy for any individual who can not afford to pay out of his or her own pocket for therapy services. Section 202(e) provides that a consent to disclose protected health information "shall not be construed as a waiver of any rights that the individual has under other Federal or State laws, the rules of evidence, or common law." However, the compelled consent to disclose information to a health plan eliminates the rights of individuals under Federal and State laws, the rules of evidence and common law with respect to those health plans.

So, will individuals in need of psychotherapy who cannot afford to pay privately retain access to effective services under subsections 202(a)(2) and (3)? Unfortunately, "reason and experience" indicate that is unlikely.

Solution—The best approach, in our view, would be to change the wording of section 202(e) as follows:

NO WAIVER.—Except as provided for in this Act, Except as provided for in this Act, Notwithstanding any other provision of this Act, an authorization to disclose protected health information by an individual shall not be construed as a waiver of any rights that the individual has under Federal or State laws, the rules of evidence, or common law.

This would make clear that the federal law is establishing a floor of protection and not eliminating protections that are based on the "reason and experience" reflected in common law and statutory law. Further, it would make sure that this section of the legislation is consistent with section 401(b) which provides:

Authorizations pursuant to sections 202 and 203 shall not be construed as a waiver of any such privilege.

Alternatively, sections 202(a)(2) and 203(a) could be revised as follows:

Section 202(a). CONSOLIDATED AUTHORIZATIONS.—A single authorization may be secured for each individual in connection with non-privileged information needed for treatment, payment, and health care operations.

Section 203(a). WRITTEN AUTHORIZATIONS.—A health care provider, health plan, health oversight agency, health researcher, public health authority, law enforcement official, employer, health or life insurer, school or university may disclose

protected health information, including privileged health information, for purposes other than those authorized under section 202, only pursuant to an authorization executed by the individual who is the subject of the information that meets the requirements of section 202(b).

This revision would permit individuals to waive the psychotherapist-patient privilege should they so desire while preserving the privilege for those who cannot afford to pay out of pocket. The failure to protect information which is subject to the psychotherapist-patient privilege from disclosure would result in health plans and other private parties routinely obtaining confidential information in the normal course of business which they would be barred from obtaining in court.

2. Health plans have few limitations on the use of identifiable information.——

Section 2(5) appropriately includes the finding that:

any disclosure of protected health information should be limited to that information or portion of the medical record necessary to fulfill the purpose of the disclosure.

Problem—Section 202(f) does not incorporate the finding, but rather

states that authorizations for treatment, payment and health care operations shall not authorize disclosures "with the intent to sell, transfer, or use protected health information for the purpose of marketing a product or service." Thus, the limitations on the use of information disclosed under the procedures of section 202 do not seem to be as broad as the finding indicates that they should be.

By contrast, section 203(e) expressly states that information disclosed under that procedure may be used or disclosed, "solely to carry out the purpose for which the information was authorized for release." Similar language appears in section 212(a).

Solution—Add the language of the finding to section 202(f) as follows:

Protected health information obtained for treatment, payment, and health care operations shall not be used for any other purpose.

3. The lack of privacy protections will cause the quality of health care operations to deteriorate.——

Section 2(6) of the bill correctly finds that:

Incentives need to be created to use non-identifiable health information where appropriate.

Problem—There is no incentive to use non-identifiable health information

under section 202 for protected information "in connection with treatment, payment, and health care operations". See section 202(a)(2). Accordingly, health plans and other private entities inevitably will compel the disclosure of health information in identifiable form without considering whether, through the use of computer technology or otherwise, they might be able to achieve their objectives by using non-identifiable information. Further, health plans will always compel the disclosure of a higher volume of identifiable health information than is needed.

HCFA's recent ill-fated effort to launch the OASIS data collection effort is an excellent example of what happens when there is no incentive to use non-identifiable health information for health care operations. The OASIS data collection effort resulted in:

(1) a loss of access to quality health care services and

(2) the collection of unreliable health information.

Effective February 24, 1999, HCFA required every patient being served by a Medicare certified home health agency, regardless of whether the services they received were paid for by Medicare or by the patient personally, to disclose to the federal and state governments more than 450 health information items about themselves at least every 60 days on an OASIS data collection form. 64 Fed. Reg. 3764. Due to immediate and strong objections from the public, Congress and the White House, HCFA suspended the project on April 27. 64 Fed. Reg. 23846.

HCFA's principal reason for launching the effort was not to make payment and coverage determinations for individual patients (indeed, many of the patients did not even seek payment and coverage from Medicare), but rather, to improve the quality of care generally by developing "overcomes measurements". Just as in this bill, patients were required to consent to the gathering and reporting of the information in identifiable form as a condition of receiving treatment from the home health agency.

It became clear in the two months the project was in effect that it was diminishing access to quality care rather than enhancing it. Many patients refused to provide the information either because it was too burdensome or too invasive of their privacy. Home health agencies then had to terminate services to the patients or face expulsion from the Medicare program. In order to prevent medically necessary services from being terminated, many of the home health nurses simply "made up" entries which were required on the OASIS data form. Thus, access to quality care deteriorated as did the reliability of the data being collected.

The privacy bill already contains a finding that the failure to protect the right to confidentiality may "reduce the willingness of patients to confide in physicians and other practitioners" in order to provide them with the information necessary for accurate diagnosis and treatment. The Senate Health, Education, Labor, and Pensions Committee has already heard testimony that physicians increasingly do not put complete information into the medical record or use less specific terminology where they are concerned that sensitive information about a patient may have to be disclosed.

Thus, it is vitally important, in the interest of preserving quality health care, that incentives be provided to use non-identifiable information where possible. For this reason, we strongly urge that "health care operations" be transferred from section 202 to section 203. Creating an incentive to use non-identifiable data where possible for the activities under "health care operations" will preserve access to quality care and enhance the effectiveness of the those activities.

It would appear that most of the activities listed in the definition of "health care operations" are designed to benefit patients generally (or limit the risk of the health plan) and are not essential to the diagnosis and treatment of the individual patient. For this reason as well, the use of non-identifiable information should be encouraged, and specific consent should be required for the use of identifiable health information. We have already seen in the ill-considered OASIS project that patients will not participate the routine collection and reporting of protected information that is not needed directly for their diagnosis and treatment.

4. The exception for self payment will force patients to forego health insurance.

As noted, the findings acknowledge that failure to protect the patient's right to confidentiality will result in the patients foregoing quality health care. Section 2(3). That finding is confirmed by the "reason and experience" noted in Jaffee v. Redmond, the recent opinion from the Health Care Financing Administration, and the recent experience with the OASIS project.

Problem—Section 202(c)(2) of the bill provides for an exception to disclosure for self-payment, but it states that the exception applies only where the individual revokes "a prior authorization for payment or health care operations described in paragraphs (1) through (6) of subsection (a) prior to a single or series of encounters with a health care provider if such individual has agreed to assume personal financial responsibility for the treatment." As currently drafted, it would appear that an individual would have to revoke the blanket authorization required by 202(a) and, therefore, revoke all health insurance coverage in order to pay privately and preserve his or her medical privacy. We understand that the intent was to allow an individual to pay privately for any item of service and thereby not be compelled to disclose information about the service to a health plan.

Solution—We suggest the following revision to subsection 202(c)(2):

An individual may exempt any item or service from the prior authorization for payment or health care operations described in paragraphs (1) through (6) of subsection (a) by not filing a claim for coverage and payment and by assuming personal financial responsibility for the item or service. The decision to assume personal financial responsibility for a particular item or service shall not affect the individual's right to seek coverage and payment for other items or services.

We would also suggest that subsection 202(b), "Requirements for Individual Authorization", include provisions that explain to the individual the consequences of not granting the blanket consent required in 202(a). That requirement currently appears in the Federal Privacy Act. Specifically, that notice should inform patients of their right to preserve their privacy by assuming personal financial responsibility for an item or service.

5. Access to quality health care should be given the highest priority.

Findings in subsections 2(7) through (10) identify the importance of timely and accurate personal health data, medical research, public health and clinical and epidemiological research. However, the findings in subsections (1) through (7) quite correctly note that quality health care cannot be provided without, first and foremost, protecting the patient's right of confidentiality. This is particularly true of psychotherapy.

Problem—Privacy legislation must clearly state that protection of the right of confidentiality which is essential for quality health care will be accorded the highest priority. Otherwise, the legislation will produce a health delivery system which is efficient, low cost and ineffective. As the Supreme Court has recognized, there is no divergence of public and private interests in the protection of confidentiality because it is an essential element of quality care.

Solution—We suggest revising the finding in subsection 2(10) to restore the priority implied in the first nine findings:

The right of confidentiality essential for quality health care must be protected when obtaining health care information for treatment, clinical and epidemiological research and public health purposes.

If we compel the disclosure of identifiable health information against the patient's will, the public's trust in the health delivery system will be destroyed, and the quality of health care and the data on which it rests will be severely and irreparably damaged.

In summary, you face important decisions, but you will not go far wrong if you simply follow the "reason and experience" suggested by the history of the issue. We look forward to working with the Committee as you move forward on this important issue.

Attachment 1

PRIVACY PRINCIPLES

American Psychoanalytic Association

March 1999

I. Privacy is essential for quality psychotherapy

A. Health information privacy is important for quality health care generally as recognized under Constitutional law, common law, state statutory law and standards of medical ethics.

1. Patients will not provide complete and accurate information to their physicians for treatment and diagnosis unless they feel confident that their communications will remain private.

2. The quality of medical research will be impaired if patients do not communicate complete and accurate information to their physicians.

B. Privacy of communications between a therapist and patient is essential, for effective psychotherapy.

II. The U.S. Supreme Court's 1996 holding in Jaffee v. Redmond (that psychotherapy communications are privileged and should not be disclosed unless the privilege is waived) should be incorporated into federal statutory law.

A. After a review of the.legal and ethical history of mental health privacy, the Court found that:

1. "Reason and experience" show that effective psychotherapy cannot be provided without a realistic expectation that therapist/patient communications will remain private;

2. Protection of mental health information privacy is consistent with both the private and public interest in access to effective psychotherapy;

3. The privacy of mental health information cannot be subject to a "balancing test" if the patient is to have confidence that the communications will be protected; and

4. All 50 states and the District of Columbia have laws protecting the privacy of communications between therapists and mental health patients.

Ill. Principles for protecting the privacy of health information.

A. Federal standards should expressly recognize that patients have a right to privacy for identifiable health information.

B. A patients right to medical information privacy should not be waived without meaningful notice and informed consent.

C. The situations in which there is an overriding, compelling public need to obtain access to medical information without the patient's consent should be rare and specified by statute which should also set forth procedural safeguards.

D. Where consent has been given for the disclosure of identifiable health information to certain entities or individuals for specific purposes, security measures should be put in place to protect against further disclosures for unauthorized purposes.

IV. Privacy standards should be designed to permit necessary uses of medical information while protecting the patient's right to privacy. Incentives should be included to encourage the use of non-identifiable health information where possible. Privacy standards should include the following:

A. Permit the use of non-identifiable health information with minimal restrictions (e.g., outcomes research, monitoring quality, peer review).

B. Require meaningful notice and informed consent for the use of identifiable health information.

C. In the rare situations, specified by statute, where identifiable health information may be obtained without the patient's consent or against the patient's will, pro-

cedural safeguards should be put into place which require those seeking the information to bear the burden of showing that:

1. There is a need for the information that directly furthers an important public interest;
2. Patient consent cannot reasonably be obtained;
3. The need can be met 9MI through the use of identifiable information; and
4. The use of the information will be limited to the purpose for which it was obtained.

For more information call Jim Pyles or Judi Buckalew at (202) 466-6650.

Attachment 2

MEMORANDUM

To: Monica Tencate
Senate Finance Committee
From: Jim Pyles
American Psychoanalytic Association
Home Health Services and Staffing Association
Date: April 30, 1999
Re: Update on OASIS Data Collection and Reporting Regulations

Attached is a copy of the HCFA notice which indicates that HCFA is delaying the mandatory collection, use, encoding, and transmission of OASIS data pending clearance by the Office of Management and Budget. OMB is focusing their review on the privacy concerns of patients at the direction of the Vice President.

This latest notice comes at the end of three weeks in which HCFA published a series of notices that have caused great confusion and disruption among home health patients and providers. Those notices were as follows:

1. April 7—HCFA put a notice to State Agencies on its Website stating that the reporting of OASIS data to the state and federal governments was being delayed pending OMB clearance but that collection of the OASIS data would proceed.
2. April 20—A revised notice was published which deleted the requirement that the OASIS data be collected.
3. April 21—Another revised notice was published stating that home health agencies were "encouraged to use the OASIS data set".

All three versions of the notice stated that what the notice really meant was that "the effective date for HHAs to begin transmitting OASIS data will be later than April 26 . . ." (Emphasis supplied.)

We repeatedly asked the question: Must home health agencies collect the OASIS data from Medicare and non-Medicare patients, and if so, must they terminate services to patients who refuse to provide the information? We never got a direct answer to that question. The attached notice (now the fourth in three weeks) was simply released on April 27.

We attended a meeting on April 28 at OMB at which HCFA officials were present. Before the meeting began, I was warned (as was the Executive Director of the Home Health Services and Staffing Association several weeks ago) that addressing the privacy issues could delay implementation of prospective payment.

In the meeting, I pointed out that our intent has never been to delay development of PPS but rather to enhance HCFA's ability to implement such a system on time and in a manner that will not destroy the effectiveness of the services being reimbursed. As evidence of that intent, I noted that I had brought the privacy concerns to HCFA's attention and offered to help develop a workable solution (a) in August of 1998, (b) in September, (c) in December, (d) in January 1999 and (e) in February 1999. Despite these efforts, HCFA failed (until April 27) to take seriously the threat to quality health care posed by OASIS.

I further pointed out that HCFA's refusal to consider the importance of medical records privacy to quality health care was surprising since the Supreme Court found in the 1996 decision in Jaffee v. Redmond, that effective mental health therapy (of the type provided by medical social workers employed by home health agencies) can only be provided if the patient feels confident that the feelings, fears and emotions that they disclose will not be communicated beyond the therapist. In effect, medical records privacy is essential for quality health care.

We have offered a solution to HCFA for months which they have failed to consider. That solution would preserve patient privacy and not jeopardize access to quality care, would enhance HCFA's chances of meeting the PPS deadline, and would minimize further disruptions for patients and home health agencies that might result from Y2K problems and changes required as a result of new legislative privacy standards scheduled for passage in August. That approach calls for HCFA to:

1. narrow the data collection effort to just Medicare patients;
2. narrow the data to be collected to just the information absolutely essential for development of a case mix adjuster for PPS (only approximately 12 out of 80 categories of information seem to fall into that category); and
3. collect only the data needed to develop the case mix adjuster in a non-identifiable manner.

Thus, there is no legitimate reason for delaying PIPS because of the need to protect the patients' right to medical information privacy.

Quality of home health services is already assured by the fact that home health agencies are subject, by statute, to the most detailed survey process of any service covered by Medicare. That process includes requirements that each patient be notified of an extensive list of rights, that the agency have a grievance procedure in place, that the agency provide each patient with a "hotline" number established by the State to receive complaints, and that agency staff have minimum levels of training. See 42 U.S.C. 1395bbb. Ironically, one of the rights that must be protected is the patients' "right to confidentiality". Section 1395bbb(a)(1)(C). Perhaps it is for this reason that HCFA did not cite any evidence of quality problems with home health services in the Basis and Purpose Statement for either the proposed or final OASIS regulations.

At the OMB meeting, we provided preliminary information which showed that OASIS, as currently designed, was acting as a barrier to quality services and was producing flawed data. Agencies have been trying to implement the OASIS data collection requirements since the February 24 effective date and have found the following:

1. Many patients strongly object to both the burdensome nature of the amount of information, which must be collected, and to the sensitive nature of the information.
2. Many patients objected strongly to the reporting of the information to the state and federal governments.
3. Many patients simply refused to answer some or all of the inquiries.

Since HCFA was taking the position that no care could be provided to a patient unless he or she consented to the collection of all of the information, many nurses were confronted with having to terminate care to patients who refused to provide even a single OASIS data item. We are finding that in those situations, the nurses will simply "make up" a response rather than force the patient to go without care. Studies have previously shown that physicians and other health care practitioners simply avoid putting certain information into clinical records or use some benign diagnosis where the patient does not want sensitive information to be reported to an insurer. Thus, it appears that the failure to protect patient privacy impairs or even destroys the reliability of the information collected.

We concur with the views expressed by OMB at our meeting that this review is likely to result in better public policy with respect to outcomes measurements.

Do not hesitate to contact me at (202) 466-6550 if you need further information. We will keep you apprised of further developments.

Attachment 3

OASIS: What's New

(From The Health Care Financing Administration Web Site)

ALERT: Delay in Mandatory Collection, Use, Encoding and Transmission of OASIS (April 27, 1999)

On April 7, we notified you that the effective date of OASIS data transmission was being delayed. In the following announcement, we would like to further clarify that collecting and encoding OASIS information is also affected. When the clearances referenced below are obtained, we will inform you here as well as publish the appropriate related notices in the Federal Register.

Delay in Mandatory Collection and Use

On January 25, 1999, we published a regulation (HCFA-3007-F, 64 FR 3764) requiring all home health agencies (HHAs) participating in the Medicare/Medicaid program to use a standardized assessment instrument, Outcome and Assessment Information Set (OASIS), for all patients. This requirement was in accordance with section 1891 of the Social Security Act, and finalized a proposed rule published March 10, 1997 (62 FR 11004). The goal of such mandatory use was so that H HAs could improve the quality of their own services to patients. Mandatory collection and use by HHAs was to begin on February 24, 1999.

In order for this mandate to be valid, we still need to obtain appropriate clearances under the Paperwork Reduction Act. The completion of this activity has been

delayed, thus delaying the requirement that HHAs must use the OASIS data set as part of their comprehensive assessment process. Upon successful completion, we will issue a notification on the HCFA Internet site (http://hcfa.gov) and publish a notice to this effect in the Federal Register.

In the meantime, we are not requiring HHAs to use the OASIS instrument. HHAs that were not meeting the requirements on or after the February 24 effective date will not be held out of compliance. Of course, given that the instrument was designed to be useful to HHAs to assess and improve the care they furnish, they may wish to use the OASIS instrument for their own purposes.

Delay in Mandatory Encoding and Transmission of OASIS Data

On January 25, 1999, we published an interim final regulation (HCFA-3006-IFC, 64 FR 3748) mandating that all HHAs participating in the Medicare/Medicaid program encode (that is, data enter) OASIS information in a standard format and transmit it to HCFA as a condition of participation. Encoding was to begin on March 26th and data transmission to the States on April 26th.

In order for this mandate to be valid, we still need to obtain appropriate clearances under the Paperwork Reduction Act, prepare and provide an individual Privacy Act notice for patients, and publish a Privacy Act notice of the existence and character of the OASIS system of records. The completion of these activities has been delayed, thus delaying the requirement that HHAs encode and transmit OASIS data. Upon their successful completion, we will issue a notification on the HCFA Internet site (http://hcfa.gov) and publish a notice to this effect in the Federal Register.

In the meantime, we are not requiring HHAs to encode and transmit OASIS data. HHAs that were not meeting the requirements on or after the above effective dates will not be held out of compliance.

Attachment 4

The Right to Medical Privacy: An Indispensable Element

of Quality Health Care

August 27, 1997

James C. Pyles

on behalf of the

National Coalition for Patient Rights

. Medical Privacy Hangs in the Balance

In a speech to the National Press Club on July 31, 1997, Secretary of Health and Human Services, Donna Shalala, announced that the growing threat to the privacy of personal medical information poses a "clear and present danger to our citizens and our health care system. [1] Noting the recent developments in genetic testing and increased computerization of vast amounts of personal medical information, Secretary Shalala stated that, "what we do over the next months, . . . could bring us great promise or even greater peril . . ."[2]

Secretary Shalala was referring to the directive contained in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA also known as the Kennedy-Kassebaum legislation) for the establishment of federal standards to protect the privacy of personal medical information for identifiable individuals. See HIPAA Sec. 264(a). That act directs the Secretary of Health and Human Services to make recommendations to Congress by August 21, 1997, and further provides that if Congress has not enacted legislation by August of 1999, the Secretary is to issue standards in regulatory form by February of the year 2000. It would appear that Congress will act well within the time frame set forth in the Kennedy-Kassebaum legislation since numerous bills purporting to protect personal medical privacy have been introduced in the last two sessions.

The Interests at Stake

Secretary Shalala noted in her recent speech that the interest at stake is "the privacy of our most cherished and personal information. . . . our family secrets". [3] She then stated, however, that "[j]ust like our free speech rights, privacy rights can

---

[1] Speech by the Honorable Donna E. Shalala before the National Press Club, at 1 (July 31, 1997).

[2] Id. at 2.

[3] Id. at 1.

never be absolute" but must be balanced against "our public responsibility to support national priorities like public health, research, quality care, and fighting fraud and abuse."

As the legal and ethical history of this issue shows, the right to medical privacy is, indeed, as fundamentally important as the constitutional right to free speech. However, such fundamental rights typically are not suspended when they conflict with national priorities. Rather, the priorities are addressed in a manner which protects the fundamental rights. [4]

It would be unacceptable under our traditional concepts of free speech for the government to prohibit newspapers from printing articles about genetic research or health care fraud simply because such research or law enforcement initiatives have been designated as national priorities. Similarly, it would be unacceptable and unwise to suspend the right to medical privacy in areas where the government has established other national priorities.

The reasons most often cited in support of the need for federal privacy standards are the increasing abuse of private medical information and the relentless assault on personal medical privacy by individuals and organizations who seek to profit from the information or seek to limit their economic risk through the use of that information. Recent examples of violations of medical privacy include managed care organizations permitting employees to have unrestricted access to all medical records of enrollees, including detailed psychotherapy notes; medical students copying medical records at night to sell to malpractice attorneys; news media publishing information from the personal medical records of political candidates; [5] a bank official serving on a state health commission using medical records to determine which bank customers had been diagnosed with cancer in order to call their loans; [6] a convicted rapist working in a hospital who harassed young girls over the telephone after obtaining their telephone numbers from their hospital medical records; [7] and pharmaceutical and medical information companies extracting information from patients' medical records in order to engage in direct marketing. [8]

To paraphrase Secretary Shalala's recent statement, the issue which must be addressed in establishing privacy standards for personal medical information is—will our health records be used to heal us or harm us? [9] The ever-lengthening list of individuals and organizations seeking personal medical information argue that they need it to promote the quality or administrative efficiency of health care. [10] As a corollary, they argue that medical privacy and quality health care represent a conflict between private and public interests which must be balanced against each other with the right to medical privacy increasingly being subjugated to the public interest in quality and efficiency. At least one federal commission and one commentator have adopted that premise without citing any support. [11]

Others have stated alternatively that the challenge is "to safeguard—not sacrifice—our privacy" and "to chart a course where individual rights and privacy would prevail. [12] So the questions arise—Is the right to medical privacy inconsistent with quality health care and does protecting the right to privacy pit the interests of the individual against the interests of the public? Current information and the history of human experience represented by constitutional, statutory and common law as well as medical ethical standards all seem to point to the conclusion that medical privacy is indispensable to quality medical care and that protection of the right to medical privacy furthers public as well as private interests.

Medical Privacy as an Essential Element of Quality Health Care: Recent Information

---

[4] The right to free speech, protected by the First Amendment to the Constitution, is "subject only to narrow and well-understood exceptions", and efforts to restrict the right are subject to "the most exacting scrutiny" by the courts. Turner Broadcasting System, Inc. v. F.C.C., 114 S. Ct. 2445, 2459 (1994).

[5] Shalala speech, supra note 1, at 1.

[6] Woodward, Computer-Based Patient Record and Confidentiality, The New England Journal of Medicine (Nov. 23, 1995).

[7] The Boston Globe (April 11, 1997).

[8] Washington Post (June 14, 1995); testimony before the Massachusetts Health Care and Insurance Committees (March 9, 1997); Pharmaceutical Executive (March 1996).

[9] Shalala speech, supra note 1, at 3.

[10] The Institute of Medicine has observed that "the number of authorized users of the computer-based patient record is too exhaustive to list, and would parallel the complete list of the individuals and organizations associated directly or indirectly with health care. . . .". L. Gostin, Health Information Privac , 80 Cornell L. R. 451, 485-86 (March 1995).

[11] National Committee on Vital and Health Statistics, p. 1 (June 25, 1997); L. Gostin, et al., Report of the Privacy and Security of Health Information in the Emerging Health Care System, at 13, Health Matrix: Journal of Law and Medicine, vol. 5:1 (1995). '

[12] Shalala speech, p. 7. See also American Medical Association policy 320.994 and 140.989.

Recent public opinion polls reveal that 75% of Americans are concerned about the loss of their medical privacy due to the computerization of medical records.[13] Another survey showed that 85% of Americans placed protecting the confidentiality of medical records ahead of providing data on diseases and treatments.[14] Yet another survey showed that 87% of Americans believe that "laws should be passed that prohibit health care organizations from giving out medical information without first obtaining the patient's permission.[15]

Setting aside the public interest consistently reflected in surveys, what is the effect on quality health care of the real or feared loss of the right to medical privacy? In one recent study, about one-fourth of adolescents said they would not seek medical care unless their privacy and confidentiality were protected.[16] Patients generally will not provide complete and accurate medical information necessary for diagnosis and treatment if they feel that their right to privacy will not be honored and protected.[17] Physicians, in turn, have begun to avoid putting detailed information into the medical record that might be damaging to the patient because they fear that they will not be able to keep the information confidential.[18]

While the need to conduct accurate research is often cited as a reason to compel the disclosure of identifiable medical information without patient consent, it seems clear from the foregoing that preserving and protecting the right to medical privacy would be more likely to promote the accuracy of medical records needed for research than would eroding or eliminating that right. Most reputable medical researchers as well as major medical associations have concluded that the protection of the right to medical privacy is not inconsistent with, but is actually necessary for, quality medical research.[19]

The United States Supreme Court's recent decision in Jaffee v. Redmond represents perhaps one of the most thorough and careful analyses of the importance of medical privacy to quality health care.[20] After considering the arguments of the litigants and numerous "friend of the Court" briefs filed by organizations on all sides of the privacy issue, the Court decided, by a 7-2 vote, that there is a "psychotherapist-patient privilege" that protects communications between a psychotherapist and the patient from discovery in a civil lawsuit. In reaching that conclusion, the Court found that both "reason and experience" led to the conclusion that quality psychotherapy can not be provided without protecting the patient's right to privacy. In reaching its conclusion, the Court relied in part on a 1972 finding of the Judicial Conference Advisory Committee which stated, ". . . there is wide agreement that confidentiality is a sine qua non for successful psychiatric treatment."[21]

Further, the Court found that protecting and preserving the individual's right to medical privacy in that case, "serves the public interest by facilitating the provision of appropriate treatment for individuals suffering from the effects of a mental or emotional problem."[22] Thus, the Court recognized that medical privacy furthers both private as well as public interests in quality health care.

Of equal significance, the Court expressly refused to apply a "balancing test" which had been used by a lower court to determine whether the right to privacy should be protected. The Court stated:

We reject the balancing component of the privilege implemented by that court and a small number of States [footnote omitted]. . . . if the purpose of the privilege [that is, to promote quality health care] is to be served, the participants in the confidential conversation must be able to predict with some degree of certainty whether particular discussions will be protected. An uncertain privilege, or one which purports to be certain but results in widely varying applications by the courts, is little better than no privilege at all.[23]

Thus, the Court recognized that citizens must be able to rely on their rights to privacy being preserved and protected if the beneficial effect on quality is to be realized.

---

[13] Shalala speech, at 3.
[14] Louis Harris and Equifax Poll, 1993.
[15] Time/CNN Poll, 1996.
[16] Shalala speech, at 3.
[17] Report of the Task Force on Patient Privacy and Confidentiality, Massachusetts Medical Society, at 10 (Nov. 8, 1996); Shalala speech, at 3.
[18] Massachusetts Medical Society, Report on Privapy and Confidentiality, supra note 17, at 7 and 9.
[19] Id. at 11 and 20.
[20] 116 S. Ct. 1923 (1996).
[21] Id. at 1928.
[22] Id. at 1929.
[23] Id. at 1932.

So current information seems to support the conclusion that medical privacy is important to preserving the accessibility of quality health care. What can be learned from the constitutional, statutory, common law and ethical history of medical privacy?

The Right to Medical Privacy Under the Constitution, Federal and State Statutes, Common Law and Ethical Standards

In numerous decisions over at least 30 years, the United States Supreme Court has repeatedly recognized that the right to privacy is a component of the right to liberty protected by the 5th and 14th amendments of the Constitution.[24] According to our Declaration of Independence, the right to liberty is "unalienable" and therefore belongs to each individual "by virtue of being alive and human—not because society grants a liberty interest".[25] The Supreme Court has further recognized two strands of the right to privacy in the area of medical care—informational privacy (freedom from disclosure of personal information) and decisional privacy (the right to make certain decisions such as secure an abortion).[26] The informational privacy strand has been interpreted as being broader than the decisional privacy strand.[27]

A variety of federal statutes provide varying degrees of protection for the right to medical informational privacy but generally only protect against disclosures by governmental agencies or by organizations offering services (such as drug and alcohol treatment services) with federal assistance.[28] Those statutes include the Federal Privacy Act of 1974, the alcohol and drug abuse treatment statutes and section 1306 of the Social Security Act[29] Although these statutes were designed to protect individuals from government disclosure of confidential information, the protection they have offered has, in reality, been "quite limited".[30]

The Employee Retirement Income Security Act of 1974 ("ERISA") expressly forbids the retaliatory or discriminatory use of medical information, but there is substantial evidence that this prohibition has been unsuccessful in preventing employers from engaging in this type of conduct.[31] Thus, there is no federal statutory model that has proven effective in protecting the right to medical privacy. Moreover, the privacy protections which exist under federal laws, including the Constitution, only extend to incursions by governmental entities. There is no general federal legislative standard for protection of medical privacy, and no federal protection at all for violations of medical privacy by private individuals and organizations.

More than a dozen states have adopted constitutional amendments designed to protect a variety of privacy interests, and many states have adopted various types of medical privacy protections in state privacy acts, provider licensure laws and patient-provider privilege law.[32] However, testimony before Congress on April 21, 1986 revealed "the state of health information privacy protection as 'very poor' and 'unprotective of patient interests.'"[33] Further testimony concluded that federal and state law "affords meager guidance for establishing a framework for the protection of medical records."[34] One commentator has observed that the most often cited problem with federal and state privacy laws "is the lack of any national-level policy establishing a legal right of medical privacy.[35]

Throughout the history of jurisprudence in this country, courts have recognized a common law right to privacy as a principle of tort law.[36] Some courts have held that the relationship between a patient and a provider of health care is a contractual relationship which includes an implied promise that the provider will keep the patient's medical information confidential.[37] One federal court has recently held, however, that the filing of a claim for health insurance coverage waives the patient's

---

[24] See F. Chlapowski, The Constitutional Protection of Informational Privacy, 71 Boston Univ. L. R. 133, 135-145 (January 1991).
[25] Id. at 143.
[26] Id. at 146-147.
[27] Id. at 147.
[28] Gostin, Privacy and Security , supra at 13-14.
[29] D. Andresen, The Computerization of Health Care: Can Patient Privacy Survive?, Journal of Health and Hospital Law, vol. 26, No. 1, at 4 (January 1993).
[30] Id.
[31] Massachusetts Medical Society, Report on Patient Privacy and Confidentiality, supra note 17, at 15.
[32] Andresen, Computerization of Health Care, at 4-5; Gostin, Privacy and Security, supra note 10 at 14-15.
[33] Gostin, Privacy and Security , supra note 11, at 12.
[34] Id.
[35] Id. at 13.
[36] Andresen, Computerization of Health Care, supra note 29, at 6.
[37] Id.

right to privacy for all personal medical information.[38] Concerns about the ineffective protection of the right to medical privacy recently led to the enactment of a provision in the Balanced Budget Act of 1997 which would recognize and preserve the right of Medicare patients to contract privately with physicians to pay for medical services without being compelled to file a claim with Medicare.[39]

Finally, medical privacy has been accepted as an ethical obligation and the "cornerstone" of quality health care throughout 2000 years medical practice.[40] The health care provider's ethical obligation dates back at least to the Oath of Hippocrates, written between the Sixth Century B.C. and the First Century A.D. which states that "on no account" should information disclosed to a physician in the course of treatment be "spread abroad."[41] The American Medical Association's Principles of Medical Ethics require physicians to "safeguard patient confidences within the constraints of the law.[42] The American Medical Association's Council on Ethical and Judicial Affairs has issued guidelines which require the patient and the physician to consent to the release of patient identifiable clinical and administrative data to any entity outside of the medical care environment.[43] More recently, the AMA has adopted a policy which acknowledges that "there exists a basic right of patients to privacy of their medical information and records."[44] The American Hospital Association's Patient's Bill of Rights states that the patient has the right "to expect that all communications and records pertaining to his or her care will be treated as confidential by the hospital and any other parties entitled to review certain information in these records.[45]

Accordingly, the human experience reflected in the Constitutional, statutory, common law and ethical history of our system of government supports the conclusion that recognition and protection of the patients' right to medical privacy is indispensable to quality health care. As the Supreme Court has noted, quality health care is "rooted in the imperative need for confidence and trust."[46] As one respected commentator has stated, "[p]rivacy is not merely a good technique for furthering these fundamental relations [such as trust]; rather, without privacy they are simply inconceivable." (emphasis added).[47]

A Principled Approach to Protecting the Right to Medical Privacy

Few would deny that the primary goal of the health delivery system is to provide quality health care for patients rather than to provide for the administrative convenience of medical information companies or to permit health insurers or other to reduce their risk. While the right to medical privacy has been recognized traditionally as necessary for quality health care and an integral part of our basic right to liberty, that right cannot be unqualified in all circumstances. Thus, there are few who would argue that patients "should have complete control" of their medical records in all cases.[48] Citizens may lose their right to liberty if they are convicted of a crime. But citizens should not lose their right to liberty or medical privacy whenever they seek health care. The American Medical Association reached a similar conclusion when it adopted a policy which states that "[c]onflicts between a patient's right to privacy and a third party's need to know should be resolved in favor of patient privacy, except where that would result in serious health hazard or harm to the patient or others.[49]

The challenge, therefore, is to establish standards which preserve the right to medical privacy wherever individuals or organizations seek identifiable medical information for claims processing, research, law enforcement or other purposes. Those standards should be soundly based on the principles of medical privacy which have evolved throughout the constitutional, statutory, common law and ethical history of the issue in this country.

---

[38] Gould v. Durkin, 1997 U.S. Dist. LEXIS 6896 (E.D. Pa. 1997)

[39] Balanced Budget Act of 1997 (H.R. 2015), Sec. 4507.

[40] Massachusetts Medical Society, Report on Patient Privacy and Confidentiality, supra, note 17, at 8 and 10.

[41] The Computerization of Health Care, supra note 29, at 2.

[42] Id. at 3.

[43] Id.

[44] Massachusetts Medical Society, Report on Patient Privacy and Confidentiality, supra, note 17, at 7.

[45] Andresen, The Computerization of Health Care, supra note 29, at 3.

[46] Jaffee v. Redmond, 116 S. Ct. at 1928.

[47] Charles Fried, Priva , 77 Yale L.J. 475, 477 (1988).

[48] Secretary Shalala appears to mistakenly believe that this is the view of many consumers. See Shalala speech, supra note 1, at 3.

[49] Massachusetts Medical Society, Report on Patient Privacy and Confidentiality, supra note 17, at 12.

Such a principled approach to the protection of medical privacy should include the following analytical framework:

1. Express recognition of the right to medical privacy.

First and foremost, federal standards should expressly recognize that consumers have a right to privacy for personally identifiable medical information. This recognition is necessary to fill the gap left by federal constitutional and statutory laws which explicitly or implicitly recognize a fundamental right to medical privacy with respect to government actions but do not recognize that right in the context of private actions. The Kennedy-Kassebaum legislation appears to contemplate such a standard when it directs the Secretary to make recommendations for standards which address, "[t]he rights that an individual who is the subject of individually identifiable information should have." Section 264(b). The Secretary seemed to imply in her July 31, 1997 speech that both she and former Secretary Elliot Richardson have recognized that consumers possess a basic right to medical privacy.[50] However, Secretary Shalala failed to include the recognition of consumers' rights to medical privacy as one of her key principles.

Some have suggested that the federal standards should only seek to protect the "confidentiality" of identifiable medical information in the possession of the many organizations which seek it. Under such an approach, individuals and organizations could compel consumers to disclose their most personal medical information without their consent and against their will so long as they promised to keep it confidential and not discriminate. Of course, such an approach would deprive consumers of their traditionally recognized right to medical privacy and erode the quality of health care. Proposals to solve privacy violations with anti-discrimination laws just drive the abuse underground and impose a nearly impossible burden on consumers to prove that their medical information has been used to discriminate against them.

2. Meaningful notice and informed consent before consumers can be deemed to have waived their right to medical privacy.

Consumers should receive meaningful notice and provide informed consent before their rights to privacy for identifiable medical information are deemed waived by them. Consumers should not be coerced into granting broad and indefinite waivers of their right to medical privacy by making the availability of health insurance contingent on such waivers.

A federal standard requiring informed consent would help restore the trust in a confidential patient-provider relationship which numerous medical associations and the Supreme Court have found indispensable to quality health care. Informed consent is required before providers can furnish medical services to any competent adult, regardless of how useful or helpful the services might be deemed to be. No less should be required for the disclosure of medical information describing the individual's treatment or medical condition.

3.The consurneils right to medical privacy should not be limited except where there is a clear and compelling public interest prescribed by statute.

In the absence of consent, consumers' rights to medical privacy for identifiable medical information should not be abolished or impaired except in limited cases of overriding compelling public interest as set forth by statute.

Clearly there are some cases where the interest of the individual and the public in protecting medical privacy must be limited by some other public interest in gaining access to the information. For example, certain information may need to be disclosed for public health purposes such as infectious disease registries, or law enforcement authorities may need to be notified by providers in cases of suspected child abuse. In view of the importance of the right to medical privacy to quality health care and the concerted efforts of numerous special interest groups to override that right, however, circumstances where the consumer's privacy right will be limited should be prescribed in statutes enacted by our elected representatives. Even in these cases, the information to be disclosed and the use to which it can be put should be carefully limited. For example, law enforcement officials investigating suspected child abuse should not be able to comb through all of a family's medical records in search of unrelated infractions.

4. Federal Standards Should Establish a Basic Level of Protection but Should Not Preempt More Protective State Laws

In view of the fact that numerous states have constitutional measures, statutory and regulatory provisions and court-made common law that recognize and protect the right to medical privacy, federal statutes and regulations should not summarily preempt those laws. The recognized need for at least a basic level of medical privacy in order to ensure quality health care, however, would seem to make a "floor" of federal protection advisable. In fact, this approach was incorporated into the Ken-

---

[50] Shalala speech, supra note 1, at 4 and 7.

nedy-Kassebaum legislation which provides that the federal standards for medical data transfer shall not preempt state law "that relates to the privacy of individually identifiable health information." See HIPAA Secs. 262(a) and 264(c)(2).

Both the American Medical Association and the Massachusetts Medical Society have adopted principles of medical privacy based on the foregoing analytical framework.[51] Establishing such a principled framework is critically important for at least two reasons. First, it forms a consistent approach grounded in the lessons of history for the resolution of the myriad cases where demands are made for identifiable medical information. The laws which are written to address specific situations should have a consistent basis, and courts and administrative agencies should have basic principles which can be used to resolve the many cases which will not be addressed in the written law. Second, such a principled approach helps shape resolutions where the right to medical privacy is preserved while other legitimate public needs are met. Unless an analytical framework is used which recognizes and protects the right to medical privacy as a fundamental objective, that right will be devoured by exceptions. Experience has shown that entities which seek medical information will always try to compel consumers to provide them with access to as much personal medical information as possible and will try to use it for the broadest possible purposes.[52]

A Framework for Calibrating Burdens

Such a principled approach also permits a "calibration of burdens" which will provide incentives to use technological developments to preserve and protect medical privacy rather than to destroy it. Under this framework, those who seek medical information would have a strong incentive to seek ways to achieve their objectives first through the use of nonidentifiable information because that information would be subject to few, if any, privacy restrictions. Where the use of non-identifiable medical information proves impossible or impractical, organizations could then seek the use of identifiable medical information by assuming the additional burden of obtaining patient consent. Finally, in the still fewer cases where patient consent is impossible or impractical to obtain, organizations would be required to sustain the much more significant burden of showing (a) that the purpose for which the information is to be put is necessary to achieve an overriding, compelling public objective, (b) that the objective cannot be attained by using nonidentifiable information or information obtained with patient consent, and (c) that only necessary information will be obtained and that information will be used only for the limited purpose for which it was sought.

This "calibration of burdens" is similar to the approach that many courts and institutional review boards have taken in determining whether personal medical information can be used without patient consent.

Establishing such a sequence of burdens is important because consumers often do not have the resources necessary to assert and defend their right to medical privacy, and violations go unredressed with such frequency that they jeopardize the underlying right. Assuming consumers have a right to medical privacy and that its preservation is essential to quality health care, the burden should not be on consumers to preserve the right but rather on those who seek to limit or suspend it.

Penalties to Prevent the Violation of the Right to Medical Privacy

Federal and state laws addressing medical privacy set forth a broad range of penalties for violating consumers' rights to privacy. Many laws prescribe financial penalties from a few thousand to several hundreds of thousands of dollars. It is well-established, however, that violations of medical privacy often result in irreparable damage to occupations, political careers, and relationships with family and friends.[53] The unauthorized access to personal medical information has also resulted in threats of physical harm to patients.[54]

Given the significant value which vast quantities of medical information may represent, simple monetary penalties are likely to be ineffective in inspiring the kind of precautions necessary to prevent irreparable harm. An approach which has shown promise under the Medicare and Medicaid programs might be effective and relatively low cost to administer. Any individual convicted of fraud under the anti-fraud and abuse provisions of the Medicare or Medicaid programs can be excluded by the Secretary from federal and state health care programs for varying periods of time.[55] Borrowing this concept, individuals and organizations who seek to handle

---

[51] Massachusetts Medical Society, Report on Patient Privacy and Confidentiality, supra note 17, at 3 and 30.

[52] Id. at 12 and 16.

[53] Gostin, Privacy and Security, supra note 11, at 23-24.

[54] See note 6.

[55] 42 U.S.C. Sec. 1320a-7.

personal, identifiable medical information could be required to obtain a certificate of good standing from the Secretary based upon a minimal showing of their capability to protect the confidentiality of that information. Individuals and organizations which are found to have failed to adhere to privacy standards could have their certifications suspended temporarily or permanently. Simply the threat of such a sanction would probably have a "sentinel effect" that would prevent many violations.

An additional approach, which has been adopted by some states, would be to permit private causes of action by consumers whose rights have been violated with the possibility of recovering double or treble damages and attorneys' fees and costs.[56]

Conclusion

There appears to be bipartisan agreement with respect to the need to protect the right of consumers to medical privacy. Former Republican Senate Majority Leader Robert Dole observed that a "compromise of privacy" that sends information about health and treatment to a national data bank without a person's approval would be something that no American would accept.[57] Similarly, Secretary Shalala stated in her speech on July 31, 1997:

No one should have to trade in their privacy rights to get quality health care. (emphasis supplied).[58]

In fact, it appears that medical privacy is necessary for quality health care. Accordingly, a floor of federal standards that will ensure that the time-honored right to medical privacy is preserved should be the highest national health care priority.

Statement of the National Association of Insurance Commissioners

Good morning, Mr. Chairman and members of the Committee. My name is Kathleen Sebelius. I am the elected Insurance Commissioner for the state of Kansas. Also, I am the Secretary-Treasurer of the National Association of Insurance Commissioners (NAIC) and the chair of the NAIC's Accident and Health Insurance (B) Committee. I am testifying this morning on behalf of the NAIC's (EX) Special Committee on Health Insurance. I would like to thank you for providing the NAIC with the opportunity to testify today about the preemption issue surrounding the health information privacy legislation currently before Congress.

The NAIC, founded in 1871, is the organization of the chief insurance regulators from the 50 states, the District of Columbia, and four of the U.S. territories. The NAIC's objective is to serve the public by assisting state insurance regulators in fulfilling their regulatory responsibilities. Protection of consumers is the fundamental purpose of insurance regulation.

The NAIC Special Committee on Health Insurance ("Special Committee") is comprised of 45 state insurance regulators. The Special Committee was established as a forum to discuss federal proposals related to health insurance and to provide technical assistance to Congress and the Administration on a nonpartisan basis. Over the past several years, members of the Special Committee, including myself, have had the privilege of testifying before your Committee on various legislative proposals.

My testimony today will focus on three aspects of the preemption issue raised by the current federal legislation. First, I will discuss the states' recognition for the need for a minimum standard to protect the privacy of health information. Second, I will give some examples of what the states have done to ensure that health information is kept confidential, and discuss the concerns we have about the preemption language in the current federal legislation and how Congress can develop a federal minimum standard without eliminating existing state protections. Third, I will address the need for Congress to clarify the scope of any federal health information privacy legislation and to develop a way for states to measure their laws against any federal standard for compliance.

II. RECOGNIZING THE NEED FOR A FEDERAL MINIMUM STANDARD

As required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Congress must enact privacy legislation by August 21, 1999. Should Congress fail to act, HIPAA requires the Secretary of Health and Human Services to promulgate regulations by February 2000. In addition to this statutory deadline, we recognize that Congress faces pressure to enact national legislation protecting the privacy of health information because the European Union issued a privacy directive that became effective in October 1998.

---

[56] Andresen, The Computerization of Health Care, supra note 29, at 5.
[57] 41 Cong. Rec. S15578
[58] Shalala speech at 1 and 4.

The states, acting through the NAIC, understand the need for uniform standards to protect the privacy of health information. A minimum standard in this area is necessary given that health information is transmitted across state and national boundaries. The transmission of health information, as opposed to the delivery of health care services, is not a local activity. This was one of our main reasons for developing a model on this issue-The Health Information Privacy Model Act (attached).

The NAIC adopted the Health Information Privacy Model Act in September 1998. This model addresses many of the same issues that the federal legislation does, such as: (1) providing an individual the right to access and to amend the individual's protected health information; (2) requiring an entity to obtain an authorization from the individual to collect, use or disclose information; and (3) establishing exceptions to the authorization requirement. Our model was developed to assist the states in drafting uniform standards for ensuring the privacy of health information. However, because our jurisdiction is limited to insurance, and health information privacy encompasses more issues than insurance and more entities than insurers, we understand the desire for broader federal legislation.

Recognizing all of the above factors, along with the fact that all of the health information privacy bills currently before this Committee preempt state law in one fashion or another, the members of the NAIC have concluded that the privacy of health information is one of the few areas where it may be appropriate for the federal government to set a minimum standard. However, it should be noted that up until this point there has been no federal standard in place. Rather, states have been the protector of consumers in this area. Any federal legislation must recognize this fact and make allowances for it.

III. PREEMPTION A. EXISTING STATE LAWS

As this Committee is well aware, the drafting of legislation to establish standards that protect the privacy rights of individuals with respect to highly personal health information is a very difficult task. Like you, the members of the NAIC sought to write standards into the NAIC Model that would not cripple the flow of useful information, that would not impose prohibitive costs on entities affected by the legislation, and that would not prove impossible to implement in a world that is rapidly changing from paper to electronic records. At the same time, the members of the NAIC recognized the need to assure consumers that their health information is used only for the legitimate purposes for which it was obtained, and that this information is not disclosed without the consumer's consent or knowledge for purposes that may harm or offend the individual.

When developing protections for health information, Congress must recognize the impact of any federal privacy legislation on existing federal and state laws. Although we cannot fully address the impact on federal law, we do know that many state laws touch on protected health information and appear in many locations within the states' statutes and regulations. These laws do not neatly fit into a federal bill's list of exceptions. For example, privacy laws can be found in the insurance code, probate code, and the code of civil procedure. Numerous privacy laws relating to health information are also contained in the states' public health laws, which address such topics as child immunization, laboratory testing, and the licensure of health professionals. Other potential areas involve workers compensation laws, automobile insurance laws, and laws regulating state agencies and institutions. In addition, many state privacy laws only address health programs or health-related information that are unique to a particular state.

Let me give you some examples of the existing state laws that protect health information.

Kansas

In Kansas, there are laws in the Public Health Code addressing the confidentiality of information obtained by the Kansas Secretary of Health and the Environment about diabetes mellitus. (K.S.A. 65-1,116). Another law addresses the confidentiality of information obtained by the Secretary of Health and the Environment about hearing-impaired infants. (K.S.A. 65-1, 155). These state laws arguably would be preempted by some of the federal bills because of total preemption by the "related to" standard or because these conditions do not fall within the exceptions in the federal bills. Presumably, the above information would be governed by the provisions of the federal law; however, the federal privacy provisions would arguably allow the Secretary of Health and the Environment to disclose protected health information, without the consent of the individual, for public health purposes or for health research as defined under the federal bills. The disclosure provisions of the federal bills are potentially broader than the Kansas statutes, which generally require that

the information be confidential and not disclosed without the individual's consent, unless identifying information has been removed, and which require the Secretary to remove the records of a child whose parents or guardian request in writing such action.

Vermont

Vermont, like some other states, has a cancer registry. (18 V.S.A. 154, 155, 156). The Vermont statutes require the Vermont Health Commissioner to keep confidential all information reported to the cancer registry, with exceptions for the exchange of confidential information with other states' cancer registries, federal cancer control agencies and health researchers under specified conditions. The provisions of these state laws would arguably be preempted by a federal privacy law that totally preempted state law or did not include state cancer registry laws as an exception to federal preemption. Presumably, a federal privacy law would allow the Vermont Health Commissioner to disclose protected health information in situations not authorized by the state's statutes, but allowed without authorization under the federal bills' public health or research provisions.

Massachusetts

Under Massachusetts' education statutes, provisions are established for the testing, treatment and care of persons susceptible to genetically-linked diseases. (Mass. Ann. Laws ch.76, 15B). The law requires the Department of Public Health to furnish necessary laboratory and testing facilities for a voluntary screening program for sickle cell anemia or for the sickle cell trait and for such genetically-linked diseases as may be determined by the Commissioner of Public Health. Records maintained as part of any screening program must be kept confidential and will not be accessible to anyone other than the Commissioner of Public Health or to the local health department which is conducting the screening program, except by permission of the parents or guardian of any child or adolescent who has been screened. Information on the results of any particular screening program shall be limited to notification of the parent or guardian of the result if the person screened is under the age of 18 or to the person himself if he is over the age of 18. The results may be used otherwise only for collective statistical purposes. Again, this state program may be preempted by a federal privacy law because it does not fall under the federal bills' preemption exceptions. Under the federal bills this health information would be at risk of disclosure authorization under the public health or research provisions.

Connecticut

Connecticut has already enacted a privacy protection law for insurance information. (Conn. Gen. Stat. 38a-975 et seq.). This law applies to insurance institutions, agents and insurance-support organizations, and it protects health information that is collected, received or maintained in connection with insurance transactions that pertain to individuals who are residents of the state or who engage in insurance transactions with applicants, individuals or policyholders who are residents of the state. It also applies to insurance transactions involving policies, contracts or certificates of insurance delivered, issued for delivery, or renewed in the state. This law applies to life, health, disability, and property and casualty insurance, and therefore to issuers of these products. This state law would be preempted under a federal bill that used a total preemption approach. Arguably any health information held by life or health insurers may still be protected under the federal legislation; however, health information held by disability or property and casualty insurers, which is currently protected under this state law, would become unprotected under the current federal legislation. Without the opportunity for the state to implement its own laws to address these types of insurers, the health information they hold would be vulnerable to potential misuse or disclosure by those who hold it. In addition, if the federal standard were to fall short of Connecticut law in some way, the level of protection for information held by life and health insurers would be diminished.

Utah

Under Utah's Health Code, the information obtained by the Drug Utilization Review Board under the Medical Assistance Act must be treated as confidential. (Utah Code Ann. 26-18-104). The board is required to establish procedures insuring that the information is held confidential by the pharmacist. The board shall adopt and implement procedures designed to ensure the confidentiality of all information collected, stored, retrieved, assessed, or analyzed by the board, its staff, or contractors to the drug utilization review program that identified individual physicians, pharmacists or recipients. The board may have access to identifying information for purposes of carrying out intervention activities, but that identifying information may not be released to anyone other than a member of the board. The board may release

cumulative non-identifying information for research purposes. Again, the federal law could preempt this state statute because there is no exception in the federal bills for regulated drugs. In addition, the pharmacist or the board arguably could release this information under the federal legislation without authorization under the research provisions.

These examples are not meant to be construed as a definitive legal analysis of the relationship between these state laws and the federal bills. The comments are not based on an extensive review of all relevant state laws that might affect the ultimate conclusion about the interaction of the federal bills and the states' laws. However, the range of state laws relating to protected health information, and the diversity of their purposes and of the entities that they affect, are critical factors for assessing the impact of any federal preemption language.

Because state laws relating to health information and privacy are located in so many different places within each states' legal code, the length of time and complexity involved in compiling a list of these laws make it a nearly impossible task. Moreover, there is no federal or state agency or other organization that has a complete compendium of state laws that could be affected by federal privacy legislation that preempts state law. Without clear information about the laws that may be impacted by legislation, preemption must be approached with caution.

B. The Best Approach to Developing a Federal Standard

An argument will be made that the only solution to this collection of state privacy laws is a total preemption of state law. However, this "solution" is a deceptively easy response to the various state privacy laws and will most certainly result in adverse, unintended consequences. The language "any State law that relates to matters covered by this Act" could preempt literally hundreds of state laws that affect protected health information.4 Many state laws that are seemingly unrelated to health information on their face affect health information privacy and could be eliminated by a total preemption approach without any equivalent federal protection. Health information or health-related information that is currently protected will end up unprotected, and states will not be able to remedy the problem or "reprotect" the information. We offer this perspective not to "protect our turf," but rather as a caution against unintended consequences to the consumer. Because of the number and scope of the laws involved, our concerns are not limited to insurance law. We do not want Congress to reduce or eliminate any protections already in place. Preemption of state law is not a workable solution.

We believe the best approach would be to set a federal standard that does not preempt state laws that have been protecting health information for so many years. Up until now, there has been no federal standard in place, and the states have been protecting consumers. We understand the desire to establish a federal floor in this area, but it is not appropriate to preempt stronger state laws or preempt state laws that are outside the scope of the federal privacy legislation. As discussed earlier, the states have enacted privacy protections for their citizens in a variety of areas. These citizens should not lose stronger protections for their health information or lose protections granted by the states in areas not contemplated by the federal legislation.

In addition, we believe that states should be allowed to enact stronger privacy protections in the future in response to innovation in technology and changes in the use of health information. We believe the best approach would balance the need for uniformity with the recognition of the states' ability to respond quickly and to provide additional protections to their citizens. States can quickly identify the impact of any federal privacy law or any changes in the use of health information and can efficiently remedy any adverse situation. We urge Congress not to take a "broadbrush" approach to preemption that would unintentionally take away protections at the state level, eliminate the states' ability to remedy unintended consequences that result from federal privacy legislation, or prevent states from responding to future changes in technology.

IV. SCOPE OF THE LEGISLATION

In addition to adopting an approach that recognizes the privacy protections already enacted by the states and that allows states the flexibility to enact stronger privacy laws in the future, we urge Congress to draft legislation that specifically outlines the areas that Congress intends to address. Congress needs to be very specific about the scope of any federal privacy legislation. This is of particular concern since the current privacy legislation is silent on many issues affecting federal and state law. The scope should not be left ambiguous or left to the courts to decide. We believe it would be better for the protection of consumers' health information if Congress would specify what is addressed by the federal legislation as opposed

to attempting to list all of the state laws that are exempt from the federal legislation.

All of the current federal bills contain specific exceptions to the federal preemption language for certain state laws. Reviewing all of the bills, these exceptions include state laws that: (1) provide for the reporting of vital statistics such as birth or death information; (2) require the reporting of abuse or neglect information about any individual; (3) regulate the disclosure or reporting of information concerning an individual's mental health; (4) relate to public or mental health and prevent or otherwise restrict disclosure of information otherwise permissible under the federal legislation; (5) govern a minor's rights to access protected health information or health care services; (6) relate to the disclosure of protected health information or any other information about a minor to a parent or guardian of such minor; (7) authorize the collecting, analysis, or dissemination of information from an entity for the purpose of developing use, cost effectiveness, performance, or quality data; and (8) concern a privilege of a witness or person in state court.

Although each of the exceptions is appropriate and the list represents a good start at enumerating the specific categories of state laws that should not be preempted, these specific exceptions to the preemption language do not alleviate our concerns. There are other state laws that do not fit into any of the explicit categories and that would therefore be preempted by the broad scope of the general preemption language. In addition, not all of these specified exceptions are included in each of the bills. We mention this to underscore the critical importance of clearly defining the scope of what the federal legislation is addressing and the applicability of any specific privacy standard or exception. We believe it wiser and easier to define what types of health information and what state laws are within the scope of the federal legislation, rather than what types of health information and what state laws are outside of the scope of the federal legislation.

In addition, we urge Congress to outline a way in the federal privacy legislation for the states to measure their laws against any federal standard and to provide options for states to meet those requirements. In HIPAA, Congress gave the states three options in meeting the requirements of that legislation. Similar guidelines are needed in the privacy legislation. States need to be able to judge whether their state laws are stronger than the federal law in order to determine whether they need to take further action to revise their laws.

V. CONCLUSION

Establishing standards to protect the collection, use, and disclosure of health information is a very important undertaking. The growth of managed care, the increasing use of electronic information, and the advances in medical science and communications technology have dramatically increased both the availability and the importance of health information. The efficient exchange of health information will save thousands of lives. The information is critical for measuring and analyzing the quality and cost effectiveness of the health care provided to consumers. Consumer benefits from advances in health information are vast. However, the potential for misuse of this information is also vast. The information itself has become a valuable product that can be sold for significant amounts of money, and the consequences of unauthorized disclosure of health information can be potentially damaging to individuals' lives. The opportunities to exploit available health information will grow in number and value as technology and medical science advance.

As Members of Congress address this critical topic, we would urge you to recognize the importance of existing state law addressing the use of health information in many contexts. Congress should be aware of the complexity of implementing federal standards without inadvertently displacing important provisions of state law. We urge Congress not to take a "broad-brush" approach to preemption that would unintentionally take away protections at the state level, eliminate states' ability to remedy unintended consequences that result from federal privacy legislation, or prevent states from responding to future changes in technology. The scope of the preemption is a critical issue, and if not carefully constructed it could lead to unintended consequences. We urge you to recognize the impact of any privacy legislation on federal and state laws as you debate this issue. Congress must take a balanced approach that recognizes both privacy rights and the need for affordable health insurance governed through effective state regulation. The members of the NAIC would be happy to work with the Members of Congress in this area. Thank you.

Prepared Statement of the Washington Business Group on Health

I. Introduction

The Washington Business Group on Health (WBGH) has historically been a strong voice for the employer community on health care issues and remains so with a membership of 165 of the nation's largest and most innovative public and private sector employers. WBGH's members provide health care coverage for more than 39 million U.S. workers, retirees, and their families. WBGH's mission since 1974 has been to represent employers in promoting market-based, performance-driven health care delivery systems that improve the health and productivity of companies and communities.

Recognizing the seriousness of confidentiality issues and the enormous impact that legislation will have on employers, WBGH has formed a work group so that members can discuss their confidentiality concerns. This work group currently has 15 participants from 11 WBGH member companies. WBGH has asked both the work group and our Board of Directors to examine proposed confidentiality legislation for its impact on the day-to-day operations of their health-related programs and to provide feedback to inform the legislative process. We hope the information in this statement provides the basis for an ongoing dialogue between employers and lawmakers about this important issue.

II. Employer Stake in the Confidentiality Debate

WBGH is keenly aware that the Congressional debate over medical confidentiality issues will progress rapidly over the next few months and that employers have a key stake in the outcome of this debate. If authorization, record access, research, and state law preemption requirements do not recognize the complex, integrated environment in which employers' health-related plans currently operate, the effective functioning of these programs could be placed in serious jeopardy.

Passing confidentiality legislation that gives proper weight to the interests of consumers, employers, researchers, health plans, pharmaceutical companies, and others that utilize individually identifiable health information is a delicate balancing act. While employers understand and agree that any final confidentiality legislation must prevent identifiable data from being used improperly or shared inappropriately, we worry that regulations used to achieve this goal will be overly stringent and may hamper employer efforts to integrate different types of health care data, manage disability and chronic illnesses, and stimulate the development of organized systems of care.

Today's marketplace requires America's corporations to perform well and operate efficiently. At a time when very few workers are unemployed and the globalization of commerce requires companies to compete worldwide for market share, leading employers are seeking out ways to optimize the health and productivity of their employees. The cost of providing workplace health benefits (group health insurance, short and long-term disability benefits, and workers' compensation benefits) is of concern to employers, with these employee health benefits averaging 20 percent-25 percent of payroll for many companies and the price of providing health care rising an average of 7 percent annually.

However, cost is by no means the only health care benefit consideration. Cutting-edge employers have been looking beyond mere cost-containment towards a total reorganization of their health benefits and human resources programs. Increasingly, such employers are integrating and streamlining a spectrum of health-related and work/life functions to enhance quality, improve clinical outcomes, control costs, ease the burdens of benefit administration, maximize workplace productivity, and better serve beneficiaries. A full 36 percent of employers in a recent Watson Wyatt-WBGH survey indicated that they are integrating portions of their workplace health benefit plans. [1]

Unfortunately, because these innovative health efforts are so revolutionary, there is little understanding outside the corporate environment about these programs or what information must be obtained to make them work. This statement outlines some of these workplace health management practices because it is crucial that members of Congress comprehend the operation of these programs, their direct and indirect benefits, and how these programs could be inadvertently handicapped by a burdensome federal confidentiality law. Before doing so, however, the evolution of employers' use of health care information is briefly described below.

III. Evolution of Employers' Use of Health Care Information

The earliest use of health care information by employers was, quite simply, to understand costs and cost drivers. As health care costs escalated into the double digits in the late 1980s, employers began to use claims and payment data to identify the medical conditions and diseases that were most costly in terms of direct medical expenses. Armed with this information, employers developed health promotion and

---

[1] Watson Wyatt-WBGH, Creating A Line of Sight: From Benefits to Business Results, Washington Business Group on Health, 1999.

disease prevention programs such as smoking cessation programs, blood pressure screenings, and exercise programs, targeted at specific conditions such as cardiovascular disease. One of the important legacies of these early efforts are employer-sponsored prenatal education programs designed to reduce the number of low birthweight babies which can cost more than $ 100,000 for delivery and initial care.

As Dr. John Wennberg and other leading health services researchers began to identify significant geographic variation in the use of health services, employers quickly realized that health information could also be used to assess the quality of the care being delivered to their employees. For example, the Pacific Business Group on Health, a coalition of major employers in California, identified an above average C-Section rate as a quality issue in the San Francisco market and worked closely with plans and providers to bring practice in line with national norms.

Since these early efforts, employers have moved to increasingly sophisticated uses of health information and have begun to link health, disability, workers' compensation, lost-time, and absence data to more fully understand the direct and indirect costs of unrecognized and/or poorly managed health conditions. In performing these analyses, individual employee data are aggregated and correlated predominately by external data management organizations. The use of individually identifiable information is typically limited to those situations where the identity of the individual is essential to carry out a function or intervention, such as in the case of disability management or the processing of workers' compensation claims.

IV. Employer Health-related Programs and Innovative Practices

Integrated Data Management. More employers are moving to integrate their health-related databases. These consolidated databases are used to identify both cost drivers and appropriate clinical interventions. Many employers have integrated their health data management systems to identify meaningful correlations and relationships among the variables in the databases.[2] For example, companies have used their integrated health data management systems to:

- identify specific problems (compare company data with other companies, units within a company, or normative data);
- determine the impact of one program on another (e.g., link data from health risk appraisals to health insurance claims);
- model the effect of proposed changes (real cost rather than cost based on actuarial estimates);
- identify potential areas for negotiations with providers (break out unit costs from utilization data).

By combining information from their health and disability programs, employers are able to achieve tangible and important results such as: creating a work environment that prevents employees from missing work, quickly returning sick or injured employees to health and to productive work, and keeping health benefits costs in check.[3]

Disease and Disability Management. Many employers and health plans have developed proactive, targeted disease and disability management programs. These programs focus on early identification and case management techniques to ensure these conditions are properly treated. In addition, employer-sponsored health promotion activities often focus on preventive services such as health screening and education to prevent illnesses and disabilities. Employers often use population health risk assessments (i.e., health risk appraisals and/or health screenings) to target health care resources to individuals who need them most. Today's health promotion initiatives increasingly incorporate primary intervention and the day-to-day management of chronic diseases, such as asthma and diabetes.[4]

In 1993, WBGH member Black and Decker (B&D) began working with a health management firm to institute a diabetes management program for B&D employees stricken with the disease. The health management firm appointed care coordinators to work one-on-one with individual diabetics in order to educate these employees about their disease and the importance of preventative care. Coordinators also helped to ensure that the diabetics had appropriate and timely supplies (insulin and needles) to treat their condition and that they were using them correctly. The medical progress of B&D's diabetic workers was tracked on a customized database. Individually identifiable information was housed in the health management firm's database, but progress reports to Black and Decker contained only population-based in-

---

[2] Putting the Pieces Together: A Guide to the Implementation of Integrated Data Management Systems, Prevention Leadership Forum, Washington Business Group on Health, 1992

[3] Creating a Line of Sight: From Benefits to Business Results, Washington Business Group on Health-Watson Wyatt, 1999.

[4] Diabetes Management: Making the Business Case, Washington Business Group on Health, 1999.

formation. The results of B&D's diabetes management program are extremely promising. By 1997, 70% of the diabetic participants felt their overall health had improved since enrolling in the program, 19 percent reported fewer diabetes-related emergency room visits since enrolling in the program, and 13% reported fewer hospitalizations. Also 78 percent felt they possessed 75 percent-100 percent control over their glucose level, compared with only 38 percent who believed they had 75 percent-100 percent control before the diabetes management initiative began.

Health and Productivity Management. One new activity where information plays a critical role is health and productivity management. Last year, WBGH launched its Health and Productivity Management Initiative to examine the links between a workforce's health and its productivity and how employers are exploring the relationship between the two. Leading employers told WBGH that by analyzing a myriad of data about health benefits, employee attendance, and corporate workplace practices they found that: (1) absenteeism and productivity losses are often consequences of unrecognized and poorly managed health conditions; (2) health plan cost-controls may work against employer efforts to manage time-loss and other disability costs; and (3) work climate impacts an employee's health outcomes and health interventions can be used to influence work climate./[5] New metrics are now being developed to better understand and illustrate the relationship between health and productivity. None of these activities would be possible if an employer's ability to legitimately analyze identifiable information was unduly restricted.

Outcomes Measurement. Large purchasers have learned the lesson that "you can't manage what you can't measure." WBGH has been a vocal advocate of developing systems to link medical treatment to outcomes and member companies have been active participants in developing HEDIS and FACCT measures. We need to ensure that the information-gathering techniques used to develop such measurement tools are not hampered.

Organized Systems of Care. Since the early 1990s, WBGH members have advanced a vision in which health care organizations will be held accountable for continually improving the health status of the population as well as the individual in the most cost-effective manner. WBGH articulates this vision through its organized systems of care (0SC) model. These OSCs integrate the financing and delivery of care that is patient-centered, integrated across treatment settings, and provided by a multidisciplinary team of clinicians. The management and sharing of information is critical to achieving the OSC vision.[6] Information systems and technologies enable OSCs to answer key questions about the appropriateness, cost, and outcomes of care provided to members. To do this, WBGH believes OSCs should have electronically linked clinical, financial, and administrative databases. This involves the transfer of individually identifiable information.

V. Administrative and Technical Safeguards

Trust is an essential element in the relationship between patients and health care providers and between workers and their employer. WBGH companies recognize that employers must ensure that strong safeguards are in place so that confidential medical information is not misused. These safeguards should enable employees to feel comfortable sharing sensitive medical information. with appropriate providers and personnel in the doctor's office and at the worksite. Accordingly, employers use specific techniques such as encryption, organizational firewalls, and password technologies to prevent inappropriate access to individually identifiable health data. Well-defined penalties are in place to deal with any confidentiality violations.

VI. Specific Comments on Proposed Confidentiality Legislation

The three major confidentiality bills the Senate will debate this year—S. 578 sponsored by Sens. Jeffords (R-VT) and Dodd (D-CT), S. 573 sponsored by Sens. Leahy (D-VT) and Kennedy (D-MA), and Sen. Bennett's (R-UT) proposal—are comprehensive in scope and are indicative of the effort being put forth by this legislative body to meet the August 1999 HIPAA-imposed deadline to pass confidentiality legislation. Despite good intentions, there are requirements in each of these bills that would interfere with an employer's ability to accomplish both simple and more complex health-related functions. We are particularly concerned with how five issues have been dealt with in proposed confidentiality legislation: (1) how an authorization to use individually identifiable health information should be obtained; (2) narrow definitions of health care treatment, payment, and operations; (3) preemption of state confidentiality laws; (4) the time frames specified for amending individually identifiable information; and (5) new regulations for privately-funded health research.

---

[5] Investing in People for Corporate Success, Washington Business Group on Health, 1999

[6] Health Care Delivery System Reform: Distinguishing Organized Systems of Care, Washington Business Group on Health, 1995

Authorization

Employers may find that drafting a detailed authorization is both difficult and impractical. Senate confidentiality legislation requires that selected entities obtain an individual's one-time, written authorization to disclose individually identifiable health information for purposes of treatment, payment, and health care operations. This authorization must at a minimum: (1) describe the nature of identifiable information being used or disclosed; (2) identify the types of people to whom disclosures would be made; (3) describe the purpose of disclosures; and (4) be in written or electronic form. While employers agree that their workers need a basic understanding of how individually identifiable health information is used, the detailed authorization requirements in Senate confidentiality legislation may be overly burdensome and compliance may be difficult.

Employer collection of authorizations would require tremendous effort. The Senate confidentiality bills mandate that employers, not health plans, obtain the authorization to use individually identifiable health information for health care treatment, payment, and operations as a condition of enrollment. Authorization collection would be a formidable administrative task for employers.

The essential link between obtaining an authorization and health plan enrollment and disenrollment is not clear. The authorization language in the Senate confidentiality bills under discussion does not provide guidance on how major benefit questions that are of concern to employers would be resolved. These are questions such as: (1) if signing an authorization is a condition of enrollment, does this mean that if an employee refused to sign such a form he would not be enrolled in a new plan or re-enrolled in his existing plan? and (2) if a worker signed an authorization but his dependent did not, would just the dependent be denied health coverage or would the whole family unit be refused insurance? WBGH fears that if the answer to these questions were yes, then selective health plan enrollment would result. This would be impractical for corporate benefit managers. It would also lead to a dearth of health care data, which would seriously hamper workplace efforts to enhance health and productivity. In addition, employee populations would not accept selective enrollment in which some family members could be denied coverage for their failure to complete an authorization.

A third authorization issue not addressed in current legislative language is the impact of a worker's revocation of his authorization to use his individually identifiable information. Will that worker be subsequently disenrolled from the plan because the plan could not use his data for future health care treatment, payment, and operations functions after revocation? This is extremely important because neither an employer nor a health plan could practically have a beneficiary participate in health-related activities without being able to use his individually identifiable data for essential health care functions

These scenarios are quite complex, but so is the health environment in which employers operate. WBGH employers are large companies that would be required to send out authorization forms to thousands of employees. They want to be sure that any confidentiality legislation clearly defines the parameters of authorization and that these parameters do not hurt workers or the administration of corporate health programs.

The definitions of treatment, payment and health care operations are too narrow. In the Senate confidentiality bills, if an employer, insurer, or health entity wants to use identifiable information for something other than health care treatment, payment, or operations, separate authorizations must be obtained on a case-by-case basis. Therefore, the definitions attached to the terms treatment, payment, and operations are particularly important. The good news for employers and their employees is that these definitions cover a wide array of current health care practices. For instance, the term health care operations has been crafted to include many health-related functions employers and health plans currently perform such as: quality assurance and improvement activities; outcomes assessments; provider education; accreditation, licensing, or credentialing; analyzing health plan claims or health care records data; utilization review; recertification or preauthorization of services; and conducting or arranging for auditing services.

It is unclear, however, whether individually identifiable information can be used in executing sophisticated health education, disease management, or disability programs. This depends on whether such management and education activities fall under the bills' definitions of treatment, payment, or health care operations. If they do not, then employers would have to obtain additional authorizations from individuals to use their health information for these purposes, making it extremely difficult to carry out innovative health education and management programs. This is an undesirable outcome.

Another concern is that the term health care treatment, payment, and operations does not appear to include worker's compensation functions. Employers recognize that regulating workers' compensation benefits has been an area traditionally handled by states but it must be understood that the application of federal standards for all health programs but workers' compensation programs could be quite problematic. If workers' compensation activities are not included in the health care treatment, payment, and operations definition, then employers may be unable to pool health, disability, and workers' compensation data to coordinate care and benefits, facilitate payment, identify at-risk employees, recognize patterns of disability incidence, or target individuals or groups for health interventions.

Employers like WBGH member Owens Coming, for example, have experienced great success in terms of reducing both costs and lost work days when workers' compensation activities have been combined with short and long term disability functions into an integrated disability program. In 1993, Owens Coming initiated its integrated disability effort and assigned regional multidisciplinary teams to formulate and implement an individualized treatment plan for each injured or disabled employee. Since this time, the number of workers on long-term disability has decreased from 800 to 525 people and total disability costs have plummeted from $25 million to $10 million.[7] If workers' compensation activities are not covered by the definition health care treatment, payment, and operations, benefit integration and the fiscal and functional improvements integration brings about, could be put at risk.

Preemption of State Confidentiality Laws

Employers need full preemption of state confidentiality laws for effective benefits administration and data collection. Not surprisingly, large, multi-state employers have generally been supportive of a uniform federal confidentiality law, instead of state-by-state regulation. Therefore the preemption provisions in some of the more stringent confidentiality bills are disconcerting. Preemption of state laws is essential for employers who often have a nationwide web of locations and workers. If a federal, uniform confidentiality standard is not enacted, the functioning and administration of employer health-related programs could be placed in serious jeopardy.

Time frames for amending individually identifiable information may be too short. The Senate confidentiality bills all give an individual the right to request inspection, copying, and amendment of his individually identifiable health information. If a request is made by an individual to amend his protected health information and the information is found to be inaccurate, an entity has 45 days in all of the bills to: (1) amend the information; (2) make reasonable efforts to inform any person who received the inaccurate information of the amendment; and (3) inform the individual that the amendment has been made.

Employers are concerned that the specified time frame for amending individually identifiable information may be too short. Once legislation is passed giving individuals the right amend their medical records, employers and health plans will undoubtedly receive many such requests. In a 45-day time frame, it would be reasonable to expect an employer to review a petitioner's medical record, amend it if it is incorrect, and inform the petitioner that the amendment has been made. It is advantageous for both workers and employers to ensure that the right set of medical facts is on record. However, amendment language that would require employers and others holding individually identifiable information to contact anyone who may have received an individual's inaccurate information in a 45-day period could be particularly problematic. In today's integrated health care environment, many authorized parties view health care data and contacting these parties will likely take longer than 45 days.

Research

Extending federal research regulations **to private research would be harmful and unwise.** WBGH is concerned about research language that would apply the privacy rules for federally funded research to all sensitive medical information being used for either public or private research. This concern is based on two principles. First, components of the federal research oversight system have been cited for being both overtaxed and sometimes ineffective. It should not be held up as a model to be replicated. Second, if employers and others were forced to follow federal research rules for each project that used individually identifiable information, a portion of the research that has led to health improvement and productivity enhancements would come to a halt.

VII. Conclusion

It is critical that proposed confidentiality legislation not place an undue burden on employers who provide workplace health benefits. While we recognize the need

---

[7] Investing in People for Corporate Success, Washington Business Group on Health, 1999.

to prevent the misuse of individually identifiable health information, we worry that stringent confidentiality regulations will result in a health data void. If this occurs, many opportunities for improving the health and well-being of employed populations would be lost resulting in increased costs and disability and diminished productivity.

In her testimony to the Senate Labor and Human Resources Committee on September 12, 1997, Secretary of Health and Human Services Donna Shalala asked, "Will our health records to be used to heal or reveal us?" This question underscores the competing interests that Congress must weigh during the 1999 confidentiality debate. We hope that when legislators consider issues of confidentiality they will focus not only on protecting privacy, but also on understanding how employers and others use critical health information to heal individuals and maintain maximum functionality. WBGH stands ready to help Congress accomplish this task.

May 12, 1999

The Honorable JAMES M. JEFFORDS, CHAIRMAN,
Committee on Health, Education, Labor, and Pensions,
Washington, DC.

DEAR MR. CHAIRMAN: This is in response to your letter of May 3, transmitting a written question from Senator Wellstone concerning medical records privacy. The following is my response for the record.

Developing a federal floor for medical records privacy that would be high enough to offer the special protections needed for information concerning mental health treatment will require several steps. It is vitally important that federal legislation ensure that the principle espoused in all bills—that information be shared only to the degree that there is a "need to know"—becomes a reality.

Access to information in the record should be limited when it is highly sensitive. During mental health treatment, a therapist frequently takes notes which include very specific and highly personal information. This level of detail can cause untold embarrassment and harm if it is shared with others, even with other health professionals. We strongly urge that federal legislation permit the segregation of highly sensitive parts of the medical record, such as psychotherapy notes, and allow patients full autonomy to decide if, when and with whom these can be shared. This option to have greater control over a portion of the record should also be available for other highly sensitive medical areas, such as child abuse records, sexually transmitted diseases, genetic information, etc.

Second, there need to be strong requirements that information needed for health care operations be de-identified. Only in circumstances where de-identified information will not accomplish an essential task, such as in quality review of a particular case of a provider, should identified data be used. In other words, the default should be non-identified data, and a process must be in place within the health plan or provider office to determine when to permit identified information to be used.

Third, as a further protection, all individuals should have access to their own medical information and the option to amend it or append additional information. Currently, some of the bills pending before the committee allow providers and health plans to deny access on the ground that this might cause "substantial mental harm". So many people have access to this information, and its release can be so damaging, that to permit such a wide exception for denial of records to persons seeking mental health care is unwarranted. The legislation should only provide an exception to access when this might reasonably be expected to cause physical injury or endanger life.

Finally, as recommended by other witnesses, law enforcement access to records should be dependent upon judicial review.

These levels of protection would not only be of great importance to persons with mental illness, but would then also offer high protections for individuals regarding other medical information.

Thank you, Mr. Chairman and Senator Wellstone, for your concern about the privacy of mental health care information.

Sincerely,

CHRIS KOYANAGI
11Policy Director

May 6, 1999

The Honorable JAMES M. JEFFORDS, CHAIRMAN,
Committee on Health, Education, Labor, and Pensions,
United States Senate,
Washington, DC.

RE: Medical Records Privacy

DEAR SENATOR JEFFORDS: Thank you again for the opportunity to appear at the April 27 hearing before the Senate Committee on Health, Education, Labor and Pensions concerning Medical Records Confidentiality. I applaud you and your colleagues for the important and impressive work you are doing on this issue.

In your letter of April 28, you asked me to respond to follow-up questions from Senator DeWine. My response is set forth below.

1. State Mandatory Reporting Laws.

The American Bar Association's current policy on the confidentiality of health care information supports federal legislation that would ensure that personally identifiable health information is not disclosed without informed, voluntary, written authorization except for specific and limited purposes—including when disclosure is necessary to comply with applicable law. The intent behind this exception is to accommodate state statutory reporting requirements. Currently, every state requires that health information indicating child abuse and neglect be reported to a state agency (usually the department of human services). Health professionals in many states also are required by statute to report specific instances that come to their attention that involve communicable diseases, elder abuse, domestic abuse, and injuries caused by deadly weapons. In some jurisdictions, reporting of a mental or physical condition that impairs driving ability also is required. These reporting laws generally grant immunity from liability for breach of confidentiality to health professionals who release health care information in a good faith belief that there is a legal requirement to do so. In addition, these laws generally impose limitations on redisclosure by the repository government agency.

The public health protection furthered by mandatory reporting laws traditionally has been a duty of the states. Longstanding laws governing reporting, surveillance, and confidentiality vary from state to state. Nevertheless, there appears to be a general consensus among public health officials that the existing system works well, and the public appears to be supportive of current use of personally identifiable data for public health functions.

The ABA policy does not specifically address preemption of state laws, but the policy does acknowledge a need to permit disclosure to comply with applicable law. The ABA therefore would support federal health records privacy legislation that does not affect mandatory reporting laws or alter practices designed to ensure compliance with them.

Speaking for myself, I would suggest that it would be advisable to limit the preemptive effect of federal legislation—as suggested in Section 207 of S. 578, Section 205 of S. 573, and Section 2G7 of S. 881—insofar as such legislation would affect a limited class of mandatory reporting laws intended to protect individuals and public health.

2. Disclosure to Law Enforcement in Exigent Circumstances.

The ABA's policy does not specifically address health care providers, disclosure of limited patient information to law enforcement officials in hot pursuit of an alleged criminal. The impetus behind and focus of the ABA policy is the need to protect the sensitive and intimate exchange between the individual patient and his or her health care providers. Accordingly, the ABA does not purport to provide guidance about related, but distinct, questions regarding urgent law enforcement needs for more limited patient identification information. I therefore will address this question in my individual capacity.

My own response to the hypothetical situation presented by Senator DeWine is that law enforcement needs could be accommodated appropriately through more explicit understanding of the scope of "protected health information" in the proposed federal bills and a more specific definition of the bills law enforcement "hot pursuit" exception to disclosure without consent.

With specific reference to Senator DeWine's hypothetical, information about whether a hospital has treated individual(s) with a specified ailment is not "protected health information" under S. 573 or S. 578, so its disclosure to law enforcement officials would not violate contemplated legislative confidentiality protections. If law enforcement officials also were to seek the names of individuals who had received treatment for a specified ailment during a specific time period, and sufficient specificity for a warrant were still lacking, their request could be accommodated through a properly circumscribed "exigent circumstances" disclosure exception.

In S. 573, the "exigent circumstances" exception reads as follows:

"This section shall not be construed to limit or restrict the ability of law enforcement authorities to gain information while in hot pursuit of a suspect or if other exigent circumstances exist."

Interpretation of this exception must strike an appropriate balance between the need to safeguard the privacy of health information and the need to facilitate legitimate law enforcement investigations. In Senator DeWine's hypothetical, perhaps this objective could be accomplished through the hospital's disclosure only of the names of individuals (if any) who sought treatment for a gash of the arm during a specific time period. Releasing only this information in circumstances of urgent need would not significantly impact patient privacy interests. Disclosure of more detailed medical record information about the individuals' history, treatment, and condition would require a court order, warrant or subpoena, as current law dictates.

If I can be of further help, either in my personal capacity or as an ABA representative, please do not hesitate to contact me.

Very truly yours,

MICHAEL BEST & FRIEDRICH LLP,
Robyn S. Shapiro

May 13, 1999

The Honorable James M. Jeffords, Chairman,
Committee on Health, Education, Labor, and Pensions,
United States Senate,
Washington, DC.

DEAR SENATOR JEFFORDS: Thank you again for the opportunity to appear at the April 27, 1999, hearing before the Senate Committee on Health, Education, Labor and Pensions concerning Medical Records Confidentiality and to respond to Committee members' follow-up questions. The remainder of this letter responds to Senator Wellstone's questions concerning privacy of decedents' medical records.

The American Bar Association's current policy on the confidentiality of health care information does not directly or separately address the privacy of decedents' medical records. However, neither does it explicitly accommodate diminished privacy protection for medical information concerning patients who have died.

My own view, based upon my academic work and my health law experience, is that privacy of such information should be protected legislatively. Without assurance that the privacy of patient confidences will be preserved after death, patients may withhold from their physicians important information about their conditions and symptoms, and thereby adversely impact the care they receive. For that reason, most states currently require that the legal responsibility to maintain confidentiality of health information continues after the patient's death; only specified individuals (e.g. the executor, the administrator of the decedent's estate, or a spouse) are authorized to request or authorize release of medical information regarding a deceased patient.

All of the current federal legislative proposals include provisions addressed to the confidentiality of decedents' medical records. Section 212 (e) of S. 573 explicitly states that the Act's provisions would "continue to apply to protected health information concerning a deceased individual" and specifies individuals who would be able to exercise the rights of a deceased patient under the Act. Section 214 of S. 578 contains similar confidentiality provisions, but would limit the Act's privacy protection of decedents, health information to a period of two years following death. Section 212 of S. 881 also would prevent disclosure of protected health information concerning a deceased individual, but would limit the authority of the decedent's representative to exercise his or her rights under the Act to a period of two years following death. The reasons for protecting the privacy of decedents, health information do not expire in two years or in any other arbitrary time period after death. The provisions in S. 573 therefore seem most appropriate to address health information privacy concerns.

Please feel free to contact me if I can be of further help.

Very truly yours,

MICHAEL BEST & FRIEDRICH LLP,
Robyn S. Shapiro

May 5, 1999

Senator Jim M. Jeffords,
728 Hart Building,
Washington DC.

DEAR SENATOR JEFFORDS: .I appreciate this opportunity to respond to Senator Wellstone's thoughtful follow-up questions from the April 27th hearing.

Patients receiving mental health treatment, especially but not exclusively psychotherapy, often reveal their innermost thoughts, fears, fantasies, dreams, and other intensely personal information as a necessary part of their treatment. Details of such disclosures are frequently included in their medical records as an unavoidable part of documenting the nature and course of their treatment. Since patients' relationships with other people are typically an important focus of their mental health treatment, potentially embarrassing or compromising personal information about these third parties may make its way into the medical record as well. Treating clinicians will often be in direct contact with these third parties, eliciting additional information from them, contributed in the hopes of aiding the patient's treatment, that may also end up in the medical record. Some states recognize this latter situation, in part, by allowing information contributed by third parties to be expunged from copies of a record before the record is turned over to a patient. To our knowledge, however, no similar protections for third parties when the record is accessed by persons or entities other than the patient have been proposed as part of any of the bills before Congress at this time.

Patients' medical records, including their records of psychiatric treatment, may well be targets for law enforcement and other entities because of the information they contain about patients and third parties alike. The clinical experience of our members suggests that patients' concerns about disclosures of their medical record information inhibit the frankness with which they address issues of importance to them in a treatment setting, and may dissuade them from entering treatment in the first place. As the U.S. Supreme Court noted in its 1996 decision in Jaffee v. Redmond, "Effective psychotherapy depends upon an atmosphere of confidence and trust ... [D]isclosure of confidential communications made during counseling sessions may cause embarrassment or disgrace. For this reason the mere possibility of disclosure may impede the development of the confidential relationship necessary for successful treatment." The cost of such concerns are seen all around us in the suffering and economic loss caused by untreated psychiatric illness.

Sincerely,

PAUL S. APPELBAUM, M.D.

The CHAIRMAN. The committee stands adjourned.

[Whereupon, at 12:35 p.m., the committee was adjourned.]

○

CMS Library
C2-07-13
7500 Security Blvd.
Baltimore, Maryland 21244

CMS LIBRARY
3 8095 00006753 4

ISBN 0-16-058703-4
90000
9 780160 587030